

**T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**Akıllı Kart Tabanlı Uzaktan Kimlik Doğrulama
Sistemi Tasarımı**

**Esmâ ERGÜNER ÖZKOÇ
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI**

**GEBZE
2008**

**T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**Akıllı Kart Tabanlı Uzaktan Kimlik Doğrulama
Sistemi Tasarımı**

**Esmâ ERGÜNER ÖZKOÇ
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI**

**TEZ DANIŞMANI
Doç. Dr. İbrahim SOĞUKPINAR**

**GEBZE
2008**



**GEBZE YÜKSEK
TEKNOLOJİ
ENSTİTÜSÜ**

**MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ
JÜRİ ONAY FORMU**

JÜRİ

ÜYE (BAŞKAN) : İbrahim SOĞUKPINAR
Doç.Dr.

ÜYE : Hacı Ali MANTAR
Y.Doç.Dr.

ÜYE : Serdar Süer ERDEM
Y.Doç.Dr.

Gebze Yüksek Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 24/01/2008 tarih ve 2008/3 sayılı kararı ile yukarıdaki öğretim elemanlarından oluşmuş jüri tarafından düzenlenen/...../..... tarihli Tez Savunma Tutanağı neticesinde Yüksek Lisans / Doktora öğrencisi Esmâ ERGÜNER ÖZKOÇ' un çalışması GYTE Mühendislik ve Fen Bilimleri Yönetim Kurulu/...../..... tarih ve/...../..... sayılı kararıyla Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans / Doktora tezi olarak onaylanmıştır.

İMZA/MÜHÜR

ÖZET

TEZ BAŞLIĞI: Akıllı Kart Tabanlı Uzaktan Kimlik Doğrulama Sistemi Tasarımı

TEZ YAZARI: Esmâ ERGÜNER ÖZKOÇ

Uzaktan kimlik doğrulama sistemleri, sistemin kaynaklarının yasal kullanıcılarının dışındaki kişiler tarafından kullanılmasını engellemek amacıyla tasarlanmaktadır. Güvensiz ağlarda kullanılan en basit yöntem; şifreli kimlik doğrulamadır ki günümüzde birçok internet uygulaması, okul sistemleri, kütüphane sistemleri, özel şirketler, resmi kuruluşlar şifreli kimlik doğrulama kullanmaktadır. Fakat yapılan araştırmalarda sadece şifre ile kimlik doğrulamanın saldırılara açık bir sistem olduğu görülmüştür.

Uzaktan kimlik doğrulama sistemleri tasarımında sadece şifre kullanmak yerine akıllı kart ve şifre kullanılarak yapılan kimlik doğrulama yöntemleri önerilmiştir. Akıllı kartın içerdiği mikroişlemci, RAM, I/O ve ROM sayesinde aritmetik işlemleri yapabilmesi ve bazı mesajları saklayabilmesi akıllı kartın uzaktan kimlik doğrulama yöntemlerinde kullanılmasını yaygınlaştırmıştır

Bu tez çalışmasında, daha önce tasarlanan uzaktan kimlik doğrulama yöntemleri incelenmiş, bunlardan Liaw-Lin-Wu'nun 2006 yılında önerdikleri şifre ve akıllı kart kullanan uzaktan kimlik doğrulama yöntemi temel alınarak yeni bir yöntem önerilmiştir. Önerilen yöntemde diğer yöntemlerden farklı olarak eliptik eğri kriptografisi (EEC) kullanılmıştır. ECC'nin yanı sıra özetleme fonksiyonu ve tek kullanımlık sayının güvenlik özellikleri de kullanılarak mutlak güvenlik sağlayan bir yöntem geliştirilmiştir. Liaw ve diğ. yönteminin çalınan akıllı kartlar ile servis durdurma saldırıları ve yanlış şifrenin yavaş tespiti gibi sorunlarına çözüm getirilmiştir. Ayrıca önerilen yöntem, Liaw ve diğ. yöntemi, Wang ve diğ. yöntemi, Liao ve diğ. yöntemi hesaplama maliyetlerinin analizi ve karşılaştırılması, yöntemlerin java platformunda gerçekleştirilmesiyle yapılmıştır.

SUMMARY

THESIS TITLE: Smart Card Based Remote Authentication System Design

THESIS AUTHOR: Esma ERGÜNER ÖZKOÇ

Nowadays with the widespread use of the Internet, remote user authentication has become important process to provide security of the system resources. The process of authentication determines the identity of a person who attempts to access the system. Various cryptographic algorithms have been developed previously for remote user authentication by using smart card to provide better security.

One of the previously developed smart card based remote user authentication scheme is Liaw et al.'s scheme, which based on hash function. Besides their enhancements, there is some vulnerability such as inefficient wrong password detection. Denial of service attack is possible by using stolen smart card attack by adversary with their scheme.

In this thesis, a more secure solution is proposed for Liaw et al.'s remote user authentication scheme via applying elliptic curve cryptography (ECC) to improve its' security features. This is a novel approach for smart card based remote user authentication systems. Proposed scheme offers ECC for smaller key length while providing the same level security with other methods. The proposed scheme and some other schemes are implemented and simulated in java platform to better analyze computational costs.

TEŞEKKÜR

Yüksek lisans tezimde bana destek olan danışmanım Sayın Doç. Dr. İbrahim SOĞUKPINAR'a,

Kıymetli fikirlerini benden esirgemeyen, beni yalnız bırakmayan amcam Orhan Ergüner'e,

Biriciğim Duygum'a,

Dostlarım, kardeşlerim Belgin'e, Dilek'e ve Alper'e,

Ve her zaman yanımda olan, her konuda desteğini eksik etmeyen canım eşim Önder'e,

En içten teşekkürlerimi sunuyorum.

Zamansız ayrıldığım ama yanımda olduklarını bildiğim kıymetlilerim; annem, babam, Saadetim ve Sedam'a...

İÇİNDEKİLER DİZİNİ

ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
ŞEKİLLER DİZİNİ	ix
ÇİZELGELER DİZİNİ	xi
1. GİRİŞ	1
2. TEMEL KAVRAMLAR VE İLGİLİ ÇALIŞMALAR	4
2.1 TEMEL KAVRAMLAR	4
2.1.1 Özetleme Fonksiyonu Özellikleri	4
2.1.2 Zaman Mührü Kullanma Amacı	5
2.1.3 Diffie Hellman Anahtar Değişim Algoritması	5
2.1.4 Eliptik Eğri Kriptografisi (ECC)	6
2.1.5 İdeal Kimlik Doğrulama Yöntemi Özellikleri	7
2.1.6 Notasyon	8
2.2 İLGİLİ ÇALIŞMALAR	9
2.2.1 Chien-Jan-Tseng Yöntemi	9
2.2.2 Ku-Chen Yöntemi	11
2.2.3 Yoon Ryu Yoo Yöntemi	14
2.2.4 Wang Zhang Zhang Khan Yöntemi	17
2.2.5 Hwang Lee Tang Yöntemi	20
2.2.6 Yoon Ryu Yoo-2 Yöntemi	22
2.2.7 Liaw Lin Wu Yöntemi	24
2.2.8 Das Saxena Gulati Yöntemi	28
2.2.9 Liao Lee Hwang Yöntemi	30
2.2.10 Hwang Li Yöntemi	33
2.2.11 Sun Yöntemi	35
2.2.12 Lee Hwang Yang Yöntemi	37
3. ÖNERİLEN YÖNTEM	40
3.1 Kayıt Fazı	40

3.2 Doğrulama Fazı	41
3.3 Şifre Değiştirme Fazı	42
4. TEST SONUÇLARI KARŞILAŞTIRMA VE GÜVENLİK ANALİZİ	44
4.1 Hesaplama maliyeti analizi ve benzetim sonuçları	44
4.2 Önerilen Yöntemin Güvenlik Analizi	46
5. SONUÇ VE GELECEK ÇALIŞMALAR	48
KAYNAKLAR	49
ÖZGEÇMİŞ	52

ŞEKİLLER DİZİNİ

Sekil

2.1 Chien ve diğ. Yöntemi Kayıt Fazı	10
2.2 Chien ve diğ. Yöntemi Bağlantı Fazı	10
2.3 Chien ve diğ. Yöntemi Doğrulama Fazı	11
2.4 Ku-Chen Yöntemi Kayıt Fazı	12
2.5 Ku-Chen Yöntemi Bağlantı Fazı	13
2.6 Ku-Chen Yöntemi Doğrulama Fazı	13
2.7 Ku-Chen Yöntemi Şifre Değiştirme Fazı	14
2.8 Yoon Ryu Yoo Yöntemi Kayıt Fazı	15
2.9 Yoon Ryu Yoo Yöntemi Bağlantı Fazı	15
2.10 Yoon Ryu Yoo Yöntemi Doğrulama Fazı	16
2.11 Yoon Ryu Yoo Yöntemi Şifre Değiştirme Fazı	16
2.12 Wang ve diğ. Yöntemi Kayıt Fazı	17
2.13 Wang ve diğ. Yöntemi Bağlantı Fazı	18
2.14 Wang ve diğ. Yöntemi Doğrulama Fazı	19
2.15 Wang ve diğ. Yöntemi Şifre Değiştirme Fazı	19
2.16 Hwang Lee Tang Yöntemi Kayıt Fazı	20
2.17 Hwang Lee Tang Yöntemi Bağlantı Fazı	20
2.18 Hwang Lee Tang Yöntemi Doğrulama Fazı	21
2.19 Hwang Lee Tang Yöntemi Şifre Değiştirme Fazı	22
2.20 Yoon Ryu Yoo-2 Yöntemi Kayıt Fazı	22
2.21 Yoon Ryu Yoo-2 Yöntemi Bağlantı-Doğrulama Fazı	23
2.22 Yoon Ryu Yoo-2 Yöntemi Şifre Değiştirme Fazı	24
2.23 Liaw Lin Wu Yöntemi Kayıt Fazı	25
2.24 Liaw Lin Wu Yöntemi Bağlantı Fazı	25
2.25 Liaw Lin Wu Yöntemi Doğrulama Fazı	26
2.26 Liaw Lin Wu Yöntemi Oturum Fazı	28
2.27 Liaw Lin Wu Yöntemi Şifre Değiştirme Fazı	28
2.28 Das Saxena Gulati Yöntemi Kayıt Fazı	29

2.29 Das Saxena Gulati Yöntemi Bağlantı Fazı	29
2.30 Das Saxena Gulati Yöntemi Doğrulama Fazı	30
2.31 Das Saxena Gulati Yöntemi Şifre Değiştirme Fazı	30
2.32 Liao Lee Hwang Yöntemi Kayıt Fazı	31
2.33 Liao Lee Hwang Yöntemi Doğrulama Fazı	32
2.34 Liao Lee Hwang Yöntemi Şifre Değiştirme Fazı	32
2.35 Hwang Li Yöntemi Kayıt Fazı	33
2.36 Hwang Li Yöntemi Bağlantı Fazı	34
2.37 Hwang Li Yöntemi Doğrulama Fazı	34
2.38 Sun Yöntemi Kayıt Fazı	35
2.39 Sun Yöntemi Bağlantı Fazı	36
2.40 Sun Yöntemi Doğrulama Fazı	36
2.41 Lee Hwang Yang Yöntemi Kayıt Fazı	37
2.42 Lee Hwang Yang Yöntemi Bağlantı Fazı	38
2.43 Lee Hwang Yang Yöntemi Doğrulama Fazı	38
2.44 Lee Hwang Yang Yöntemi Şifre Değiştirme Fazı	39
3.1 Önerilen Yöntem Kayıt Fazı	40
3.2 Önerilen Yöntem Doğrulama Fazı	42
3.3 Önerilen Yöntem Şifre Değiştirme Fazı	43

ÇİZELGELER DİZİNİ

Çizelge

2.1 Notasyon	8
4.1 Hesaplama Maliyetlerinin Karşılaştırılması	45
4.2 Hesaplama Maliyetleri Test Sonuçları	45

1. GİRİŞ

Uzaktaki bir sistemin kaynaklarına erişim için kullanıcıların giriş izinlerinin olması gerekmektedir. Bu amaçla güvensiz ağlarda kullanılan en basit yöntem; şifreli kimlik doğrulama'dır. Bu yöntem ile güvenliğin temel ilkelerinden olan bütünlük ve güvenilirlik sağlanmaktadır. Birçok internet uygulaması, okul sistemleri, kütüphane sistemleri, özel şirketler, resmi kuruluşlar şifreli kimlik doğrulama kullanmaktadır. Ancak günümüz koşullarını ele alırsak sadece şifre ile kimlik doğrulamanın saldırılara karşı zayıflıkları olduğu açıktır. Bu sebepten dolayı kimlik doğrulama için birçok araştırma yapılmış ve çok sayıda yöntem önerilmiştir.

Kimlik doğrulamanın bilinen en kolay yöntemi, kullanıcının tanımlayıcısı(ID) ve şifresi ile sistemin kaynaklarına erişmesidir. Bu yöntemde sistemin kaynaklarına erişmek isteyen kullanıcı ID ve şifresini(PW) güvensiz ağ üzerinden uzak sisteme iletir; sunumcu tarafında tutulan ID ve şifre tablosunda, kullanıcının girdiği ID aranır; bulunursa girilen şifre ile tablodaki şifre karşılaştırılır, eşleşirse kullanıcıya sistemin kaynaklarına erişim izni verilir.

Sunumcudaki tutulan şifre tablosu [Lamport, 1981], şifrenin çalınması saldırıları, değiştirme saldırılarını, servis durdurma saldırılarını kolaylaştırır. Ayrıca sistemin milyonlarca kullanıcısının olduğu düşünülürse, sistemde fazla yükleme olması ve tablonun bakımının güçleşmesi tablo kullanmanın diğer dezavantajlarıdır. Yapılan araştırmalar sonucunda bu probleme en iyi çözümün sunumcu tarafında bir doğrulama tablosu tutulmaması olduğuna karar verilmiştir. Ve sunumcudaki doğrulama tablosu tutulmayan yöntemler geliştirilmiştir.

Fakat geliştirilen bazı yöntemlerde [Hwang & Li, 2000] kullanıcıya şifresini seçme ve değiştirme hakkı verilmemiştir. Daha sonraki çalışmalarda [Liaw, Lin & Wu, 2006], [Wang ve diğ. 2006] kullanıcıya şifresini seçme ve istediği zaman değiştirebilme olanağı tanınmıştır. Geliştirilen yöntemlerin kullanıcıya verdiği imkânların yanı sıra güvenliği de sağlamaları gerekmektedir. Yalnızca uzak sistemin kullanıcıyı doğrulamasıyla yetinmeyen kullanıcının da uzak sistemi doğrulamasını yani iki taraflı

doğrulama yapan yöntemler önerilmiştir [Liaw, Lin & Wu, 2006], [Wang ve diğ. 2006], [Liao, Lee & Hwang–1, 2005], [Yoon, Ryu & Yoo, 2005].

Genel olarak uzaktan kimlik doğrulama çağımızın en önemli güvenlik gereksinimlerindendir. Bu sebeple uzaktan kimlik doğrulama için birçok yöntem geliştirilmiştir. Bu yöntemlerde mutlak güvenliği sağlarken performanstan ödün verilmiş ya da performansı arttırırken mutlak güvenlik sağlanamamıştır. Genel olarak önerilen bu yöntemlerini sınıflandırılırsa [Liao, Lee & Hwang–2, 2006];

- Bir şeyler bilerek kimlik doğrulama örneğin; Şifre
- Bir şeylere sahip olarak örneğin; Akıllı Kart
- Bazı karakteristik özellikleri kullanarak örneğin; Parmak izi

Sistemin güvenliği, bu yöntemler farklı kombinasyonlarla kullanılarak arttırılabilir. Son zamanlarda üzerinde en çok araştırma yapılan kombinasyon akıllı kart ve şifre kullanarak yapılan kimlik doğrulama yöntemidir. Akıllı kartın içerdiği mikroişlemci, RAM, I/O ve ROM sayesinde aritmetik işlemleri yapabilmesi ve bazı mesajları saklayabilmesi akıllı kartın uzaktan kimlik doğrulama yöntemlerinde kullanılmasını yaygınlaştırmıştır. Böylece uzak sistemde, bir tablo tutulmasına gerek de kalmamaktadır.

Akıllı kart ve şifre kombinasyonu ile geliştirilen bu yöntemlerin [Liao, Lee & Hwang–2, 2006],[Tsai, Lee,& Hwang, 2005], [Liao, Lee & Hwang–1, 2005], [Yoon, Ryu & Yoo, 2005],[Lee, Hwang & Yang 2002] güvenliği kriptografi esastır. Yöntemler kullandıkları kriptografik algoritmaya göre şu şekilde sınıflandırılabilir [Tsai, Lee,& Hwang, 2005];

- Özetleme Fonksiyonu tabanlı;
- RSA tabanlı
- El-Gamal tabanlı

Geliştirilen bazı yöntemler bu kriptografik algoritmalara yardımcı olarak zaman mührü veya tek kullanımlık sayı kullanmaktadırlar [Liao, Lee & Hwang, 2005], [Yoon, Ryu & Yoo, 2005], [Wang ve diğ., 2006]. Sebebi, kullanıcı mesajını uzak sisteme iletirken kötü niyetli kişiler tarafından mesajın ele geçirilip daha sonra yasal kullanıcıymış gibi uzak sisteme gönderme yani tekrarlı gönderme saldırılarına karşı yöntemi korumaktır. Fakat zaman mührü kullanımı yanında zaman senkronizasyonu problemini de getirmiştir. Bu sebepten tek kullanımlık sayı esaslı yöntemler daha çok tercih edilmektedir.

Bu tez çalışmasında yukarıda bahsi geçen yöntemlerden farklı olarak eliptik eğri kriptografisi (EEC), özetleme fonksiyonu ve tek kullanımlık sayının güvenlik özelliklerini kullanarak mutlak güvenlik sağlayan bir yöntem önerilmiştir. Önerilen yöntem Liaw-Lin-Wu'nun 2006 yılında önerdikleri yöntem temel alınarak oluşturulmuştur. Liaw yönteminin çalınan akıllı kartlar ile servis durdurma saldırıları ve yanlış şifrenin yavaş tespiti gibi sorunlarına çözüm getirilmiştir.

2. TEMEL KAVRAMLAR VE İLGİLİ ÇALIŞMALAR

Bu kısımda uzaktan kimlik doğrulama yöntemlerinde kullanılan temel kavramlara ve sahip olması gereken özelliklere yer verilecektir.

2.1 TEMEL KAVRAMLAR

2.1.1 Özetleme Fonksiyonu Özellikleri

Bir özetleme fonksiyonunun $-h(.)$ - sahip olması gereken temel özellikler;

[1] Girdi 'M' herhangi uzunluktaki bir veri bloğu olabilmelidir.

[2] Sabit uzunlukta bir çıktı verir (*compression, expansion*).

[3] Verilen herhangi bir M için, $h(M)$ 'nin hesaplanması kolay olmalıdır.

Kimlik doğrulama yönteminde kullanılan özetleme fonksiyonunun sahip olması gereken özellikler;

[4] Tek yönlü olması gerekmektedir; bir özetleme çıktısı h , için $h(x)=y$ den x 'i hesaplamak kolay olmamalıdır (*pre-image resistance*).

Pre-image saldırısı; Verilen bu özelliğe karşı yapılan saldırıdır ve 2^n adım gerektirir. Burada n girdi büyüklüğünü temsil etmektedir. Örneğin seçtiğimiz özetleme algoritması MD5 ve girdi 128 bit olduğu durumda saldırganın 2^{128} kez özetleme fonksiyonunu denemesi gerekmektedir.

[5] $h(x)=h(y)$ özelliğini gösteren herhangi (x,y) veri ikilisi kolaylıkla bulunamamalıdır (*collision resistance*).

Doğum günü saldırısı (Birthday attack); Bu özelliğe karşı geliştirilen saldırıdır ve $2^{n/2}$ adım gerektirir. Yukarıdaki örnekte saldırganın 2^{64} kez özetleme fonksiyonunu denemesi gerekmektedir.

2.1.2 Zaman Mührü Kullanma Amacı

Zaman mührü $| \text{Saat}-T | < T_1 + T_2$ olup olmadığını kontrol ederek yöntemi tekrarlı gönderme saldırılarına karşı korumak amacıyla kullanılır. Yani kriptografik olarak eklendiği mesajın yeni olup olmadığını anlamaya yardımcı olur.

Saat; Alıcının yerel zamanı

T_1 ; Gönderici ve alıcı arasındaki normal yerel saat farkı

T_2 ; Tahmin edilen Ağdaki gecikme süresi.

Zaman mührü kullanmanın dezavantajı zaman senkronizasyonu problemidir.

2.1.3 Diffie Hellman Anahtar Değişim Algoritması

1976 de Diffie ve Hellman güvensiz ağlarda iletişim kurmak isteyen iki tarafa ortak bir anahtar ile güvenli iletişim imkânı tanıyan algoritma önermişlerdir. Algoritma ayrık logaritmik problemin çözümünün zorluğunu temel alır. Haberleşmek isteyen A ve B için sırasıyla g ve p açık parametreler (p asal, $g < p$ ve g , p 'nin primitif kökü) olmak üzere algoritma adımları şu şekildedir:

- A rasgele büyük bir sayı α seçer ve B ye

$$A = g^{\alpha} \mod p \quad (2.1)$$

gönderir.

- B de rasgele büyük bir β sayı seçer ve A ya

$$B = g^{\beta} \mod p \quad (2.2)$$

gönderir.

- Sonra her iki tarafta oturum anahtarını üretir

$$K = B^{\alpha} \mod p = A^{\beta} \mod p = g^{\beta \cdot \alpha} \mod p \quad (2.3)$$

Bu şekilde α ve β bilinmeden kimse oturum anahtarını hesaplayamaz.

2.1.4 Eliptik Eğri Kriptografisi (ECC)

Eliptik eğriler $E_p(a,b)$ olarak ifade edilirken eğri denklemini (2.4) sağlayan noktaların bir kümesini temsil eder. Kriptografideki eliptik eğriler, üzerindeki noktalar ile işlem yapılarak -noktanın kendisiyle aynılanması veya başka bir nokta ile toplanması- kullanılmaktadır. $Q = k.P$: P noktasının k defa kendisiyle aynılanması sonucu eğri üzerinde Q noktası hesaplanmasını ifade eder (*scalar point multiplication*). ECC'nin güvenilirliği eliptik eğri ayrık logaritmik probleminin zorluğuna dayanır(ECDLP).Tüm eliptik eğriler güçlü güvenlik özelliklerine sahip değildir. Bu sebeple NIST tarafından güvenilir eğrilerin listesi verilmiştir [NIST,1999]. ECC diğer kriptografik tekniklere kıyasla daha küçük boyuta ve daha hızlı anahtar üretimi sağlarken güvenlikten ödün vermediği için tercih edilir. Burada eliptik eğri denkleminin yanı sıra önemli bir parametre de $G(x, y)$ taban noktasıdır ki her bir eliptik eğri için sabittir. Bu noktanın sırası (order) “n” ve eliptik eğri kriptosisteminde “k” n’den küçük, rasgele bir sayı olarak seçilir ve gizlidir, $G(x, y)$ ve $E_p(a,b)$ ise herkes tarafından görülebilmektedir (public). $P=k.G$ işlemi ile P açık anahtarı hesaplanır. Çünkü $P = k.G$ denkleminde P ve G bilinse dahi k’nın hesaplanması verimli değildir (ECDLP). Yukarıdaki bilgiler ışığında aşağıda önerilen yöntemde kullanılan Eliptik Eğri Diffie Hellman kriptografik yöntemi özetlenmiştir.

$$y^2 = x^3 + ax + b \mod p \quad (2.4)$$

Eliptik Eğri Diffie Hellman (ECDH)

ECDH kullanarak haberleşmek isteyen ikili A ve B,

- 1- Aynı eliptik eğri parametrelerini - $E_p(a,b)$, $G(x, y)$ - kullanacaklarına mutabık olmalıdırlar.
- 2- Kendi gizli anahtarlarını üretmelidirler; N_A, N_B
- 3- Açık anahtarlarını hesaplamalıdırlar(2.5) ve birbirlerine göndermelidirler.

$$P_A = N_A \cdot G, \quad P_B = N_B \cdot G \quad (2.5)$$

4- Her iki tarafta karşı tarafın açık anahtarıyla kendi gizli anahtarını çarpmalıdır (2.6), (2.7);

$$K_A = N_A \cdot P_B \rightarrow K_A = N_A \cdot N_B \cdot G \quad (2.6)$$

$$K_B = N_B \cdot P_A \rightarrow K_B = N_B \cdot N_A \cdot G \quad (2.7)$$

5- Böylece her iki tarafta da ortak $K_A = K_B$ anahtarı hesaplanmış olur.

2.1.5 İdeal Kimlik Doğrulama Yöntemi Özellikleri

Yapılan çalışmalar sonunda birçok yöntem geliştirilmiş ve doğrulama için şifre kullanan mükemmel bir uzaktan kimlik doğrulama yönteminde olması gereken özellikler belirlenmiştir Bunlar [Liao, Lee & Hwang, 2006], [Tsai, Lee & Hwang 2005];

Ö1- Sunumcu tarafında herhangi bir şifre veya doğrulama tablosu saklanmamalıdır.

Ö2- Şifre kullanıcı tarafından seçilebilmeli ve istendiği takdirde kolaylıkla değiştirilebilmelidir.

Ö3- Şifre sistem yöneticisi tarafından görülmemelidir.

Ö4- Şifreler düz metin halinde güvenli olmayan ağda iletilmemelidir.

Ö5- Şifre akılda kolay tutulacak uzunlukta olmalıdır.

Ö6- Yöntem hesaplama kolaylığına sahip ve çalışma zamanı konusunda verimli olmalıdır.

Ö7- Kullanıcının yanlış şifre girdiği kolaylıkla tespit edilebilmelidir.

Ö8- İletişimin güvenilirliğini sağlamak için oturum anahtarı üretimi doğrulama fazında olmalıdır.

Ö9- Kullanıcının bağlantı mesajında kısmi kayıpları önlemek amacıyla ID dinamik olarak her bağlantıda değişmelidir.

Ö10- Sunumcunun gizli anahtarının kaybolması veya çalınması durumunda dahi yöntem güvenilir olmalıdır.

2.1.6 Notasyon

Bu kısımda tezde kullanılan şekiller ve notasyonların ne anlama geldikleri gösterilmektedir.

Çizelge 2.1 Notasyon

PW	Kullanıcı şifresi
ID	Kullanıcının tanımlayıcısı
S	Uzak sistem
$h(.)$	Tek yönlü özetleme fonksiyonu
$h_k(.)$	Tek yönlü anahtarlı özetleme fonksiyonu
$\oplus$	Mantıksal harici veya operasyonu
X	S'nin gizli anahtarı
N_i	Kullanıcının rasgele ürettiği tek kullanımlık sayı (Tek kullanımlık sayı)
N_s	S'nin rasgele ürettiği tek kullanımlık sayı (Tek kullanımlık sayı)
P_i	Kullanıcının açık anahtarı
P_s	Uzak sistemin açık anahtarı
K_i	Akıllı kartta üretilen oturum anahtarları
K_s	S de üretilen oturum anahtarları
T_u	Kullanıcının o anki zamanı
T_s	Uzak sistemin o anki zamanı

2.2 İLGİLİ ÇALIŞMALAR

Bu bölümde Literatürde daha önceden geliştirilmiş akıllı kart kullanan uzaktan kimlik doğrulama yöntemlerinde yer verilecektir.

Genel olarak yöntemler üç ana fazdan oluşmaktadır. Bunlardan ilki sistemin kaynaklarını kullanmak isteyen kişinin sisteme tanıtılmasını, kayıt olmasını sağlayan “Kayıt fazı”dır. Kayıt fazı her kullanıcı için sadece bir kez ve güvenli ağ üzerinde gerçekleştirilir. Sisteme kaydolun kişi (kullanıcı), sistemin kaynaklarına erişmek için sisteme bağlanması gerekmektedir bu kısımda da “Bağlantı fazı” devreye girmektedir. Kullanıcının sistemi, sisteminde kullanıcıyı doğruladığı kısım ise “Doğrulama fazı” olarak adlandırılmıştır. Kayıt fazı dışındaki fazlar güvensiz ağlarda gerçekleştirilmektedir. Bu üç ana faz bazen bağlantı ve Doğrulama fazının birleşmesiyle ikiye de düşebilmektedir. Ayrıca bazı yöntemler kullanıcının şifresini değiştirme imkanı verdiği için Şifre değiştirme/ güncelleme fazı da ana fazlara eklenmiştir. Bu bölümde verilecek olan yöntemler faz temelli işlenecektir.

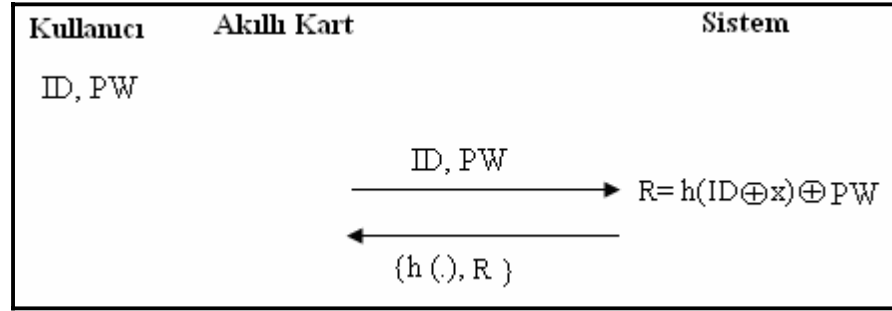
2.2.1 Chien-Jan-Tseng Yöntemi

2002 yılında Chien ve diğ. tarafından geliştirilen yöntem [Chien, Jan & Tsang, 2002], Kayıt, Bağlantı ve Doğrulama olmak üzere üç fazdan oluşmaktadır.

Kayıt Fazı;

- 1- Kullanıcı tanımlayıcısını (ID) ve şifresini (PW) güvenli ağda uzak sisteme (S) iletir.
- 2- ID ve PW alan S, gizli anahtarı x 'i kullanarak R' yi Şekil 2.1 de gösterildiği gibi hesaplar.
- 3- S kullandığı özetleme fonksiyonunu ve hesapladığı R değerini akıllı kartın hafızasına kaydeder.

Kayıt fazı sonunda akıllı kartı kullanıcıya teslim edilir.

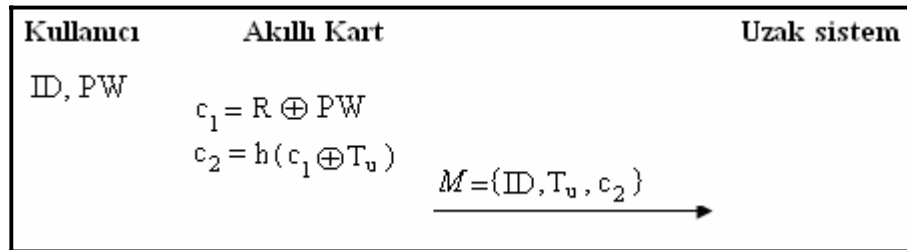


Şekil 2.1 Chien ve diğ. Yöntemi Kayıt Fazı

Bağlantı Fazı;

Kullanıcı sisteme bağlanmak istediğinde;

- 1- Akıllı kartını sistemin kart okuyucusuna yerleştirir ve ID, Şifre ikilisini tuşlar.
- 2- Akıllı kartta c_1 ve c_2 değerleri Şekil 2.2 de ki gibi hesaplanır.
- 3- Kullanıcının tuşladığı ID, o anki zaman mührü T_u ve hesaplanan c_2 değeri uzak sisteme gönderilir.



Şekil 2.2 Chien ve diğ. Yöntemi Bağlantı Fazı

Doğrulama Fazı;

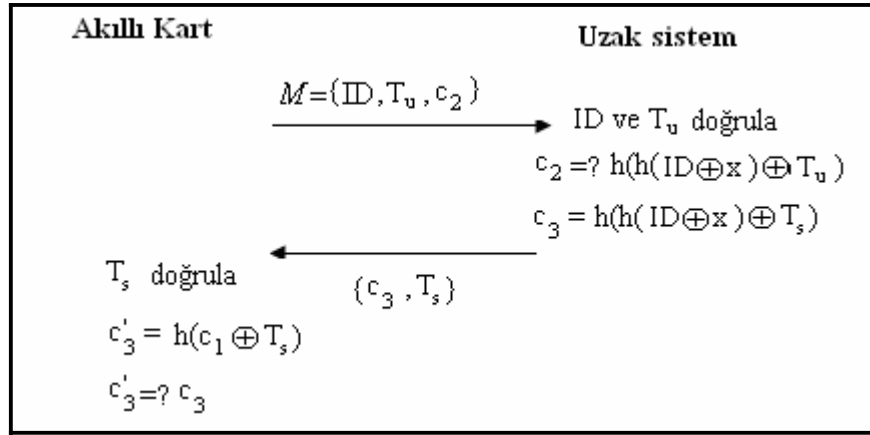
Uzak sistem kullanıcının bağlantı mesajını -M- aldığı anda doğrulama fazı başlar. S sırasıyla aşağıdaki işlemleri gerçekleştirir (Şekil 2.3):

1. ID ve T_u 'nun geçerliliği sorgulanır, geçerli ise 2. adıma geçilir aksi halde bağlantı isteği reddedilir.

2. S Şekil 2.3 de ki gibi c_2 ' yi hesaplar ve M de gönderilen c_2 ile karşılaştırır, eşitse uzak sistem kullanıcıyı doğrulamış olur. Kullanıcının da S yi doğrulaması için sistemin o anki zamanı T_s ile c_3 hesaplanır. T_s ve c_3 akıllı karta gönderilir.

3. Mesajı alan akıllı kart, T_s 'nin geçerliliğini sorgular geçerli ise c_3 ' hesaplar ve gönderilen ile karşılaştırır aynı ise kullanıcı uzak sistemi doğrulamış olur.

Doğrulama fazı sonunda kullanıcı uzak sistemin kaynaklarına yetkisi dâhilinde erişebilir ve kullanabilir.



Şekil 2.3 Chien ve diğ. Yöntemi Doğrulama Fazı

2.2.2 Ku-Chen Yöntemi

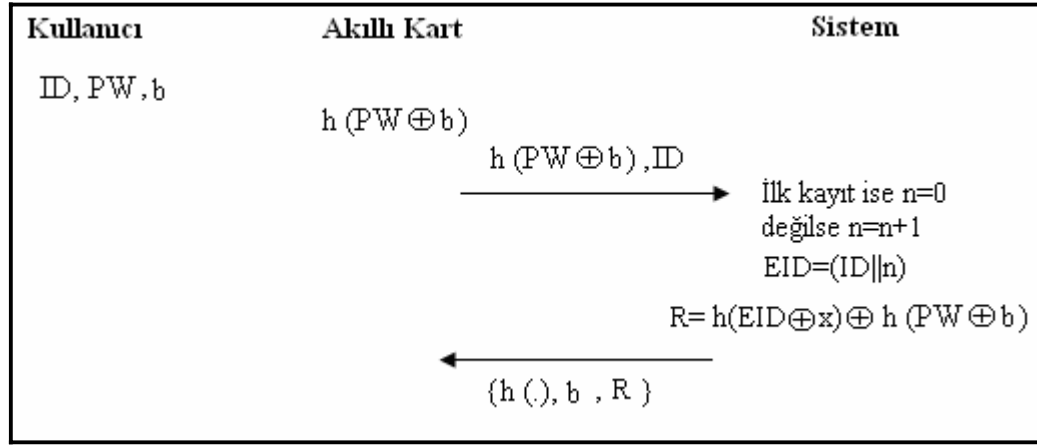
Chien ve diğ.'nin önerdikleri yöntemin zayıflıklarını gidermek için Ku-Chen'in 2003 yılında önerdikleri yöntemdir[Ku &Chen, 2004]. Kayıt, Bağlantı, Doğrulama ve Şifre değiştirme olmak üzere 4 fazdan oluşur.

Kayıt Fazı;

Bu faz kullanıcı ID ve PW ikilisinin yanında rasgele seçtiği b sayısını tuşlamasıyla başlar ve aşağıdaki gibi devam eder (Şekil 2.4):

1. Akıllı kartta, girilen şifre ve b değeri XOR operasyonuna tabi tutulduktan sonra özet fonksiyonundan geçirilir. Hesaplanan değer ve ID, S'ye gönderilir.

2. Mesajı alan S, kullanıcının daha önceden sisteme kaydolup olmadığını “n” değişkeni yardımıyla kontrol eder. (Şekil 2.4)
3. ID ve n değerini birleştirerek EID oluşturulur. Oluşturulan EID ile Şekil 2.4 deki gibi R hesaplanır.
4. Hesaplanan R değeri, kullanıcı tarafından seçilen b ve kullanılan özet fonksiyonu akıllı karta yazılır.

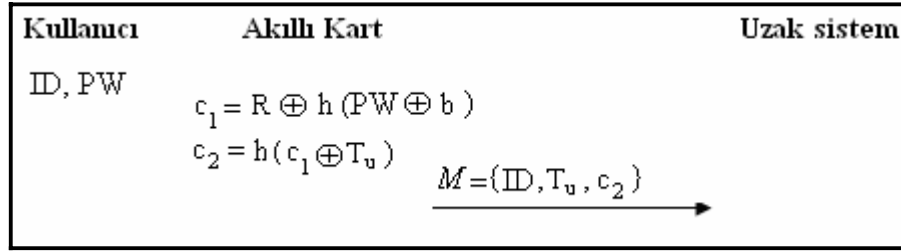


Şekil 2.4 Ku-Chen Yöntemi Kayıt Fazı

Bağlantı Fazı;

Kullanıcı sisteme bağlanmak istediğinde;

1. Akıllı kartı, kart okuyucusuna yerleştirir, ID ve PW ikilisini sisteme girer.
2. Akıllı kart c_1 ve c_2 değerlerini Şekil 2.5 deki gibi hesaplar.
3. Kullanıcın o anki zamanını T_u , hesaplanan c_2 değerini, ID ile birlikte uzak sisteme gönderir.



Şekil 2.5 Ku-Chen Yöntemi Bağlantı Fazı

Doğrulama Fazı;

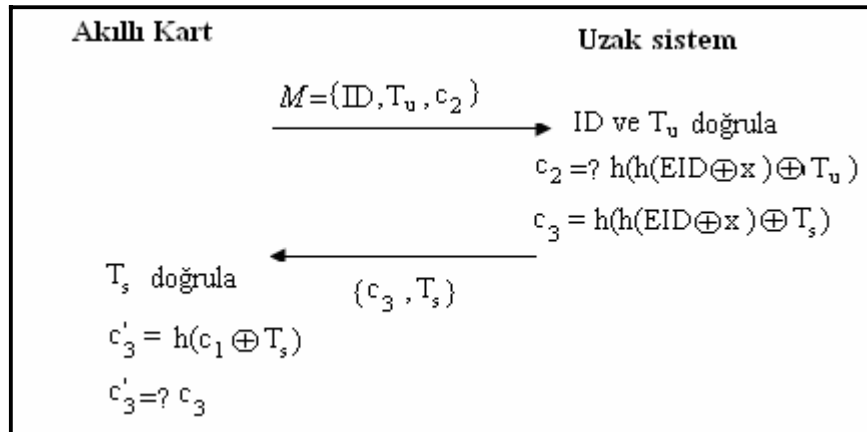
Uzak sistemden mesaj Doğrulama fazında alınır. Bu faz Chien ve diğ. yönteminin doğrulama fazıyla çok benzerlik gösterir (Şekil 2.6).

1. ID ve T_u 'nun geçerliliği sorgulanır, geçerli ise 2. adıma geçilir aksi halde bağlantı isteği reddedilir.

2. S Şekil 2.6 da ki gibi c_2 ' yi hesaplar ve bağlantı mesajında gönderilen c_2 ile karşılaştırır, eşitse uzak sistem kullanıcıyı doğrulamış olur. Kullanıcının da S yi doğrulaması için sistemin o anki zamanı T_s ile c_3 hesaplanır. T_s ve c_3 akıllı karta gönderilir.

3. Akıllı kart, T_s 'nin geçerliliğini sorgular geçerli ise c_3 ' hesaplar ve gönderilen ile karşılaştırır aynı ise kullanıcı uzak sistemi doğrulamış olur.

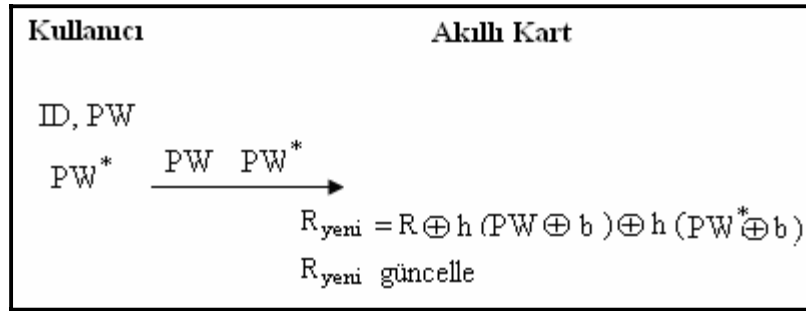
Doğrulama fazı sonunda her iki tarafta birbirini doğrulamış olur.



Şekil 2.6 Ku-Chen Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Chien ve diğ. yönteminde bulunmayan bu faz, kullanıcıya şifresini kayıt fazından sonra istediği zaman değiştirebilmesi imkanı verir. Bu fazda öncelikle kullanıcı var olan şifresini ve ID' sini girer, daha sonra şifre değiştirme isteğini sisteme bildirir ve Yeni şifresini (PW^*) girer. Akıllı kartta PW^* ile yeni değerler Şekil 2.7 de gösterildiği gibi hesaplanır. Ve akıllı kartta var olan eski şifre ile hesaplanmış değerler yenisiyle güncellenir.



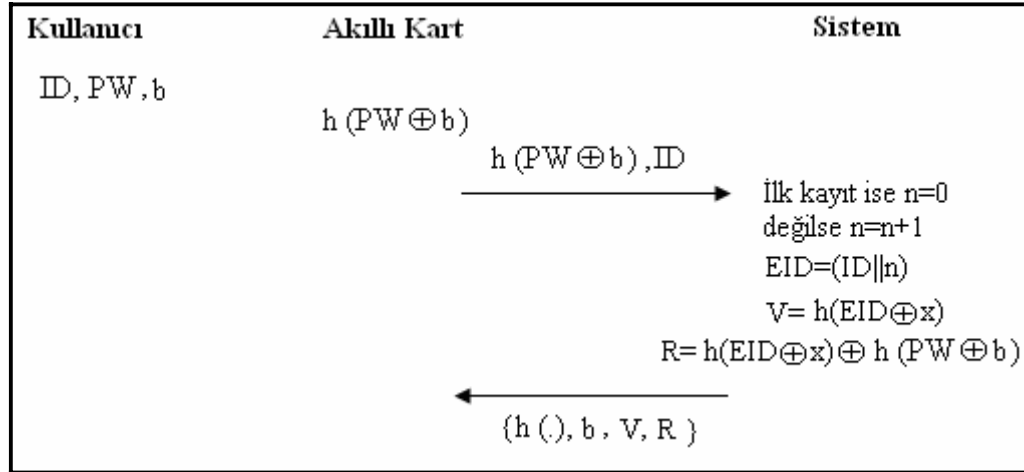
Şekil 2.7 Ku-Chen Yöntemi Şifre Değiştirme Fazı

2.2.3 Yoon Ryu Yoo Yöntemi

Ku-Chen yönteminin de yeteri kadar güvenli olmadığı Yoon-Ryu-Yoo tarafından ispatlanmıştır [Yoon, Ryu & Yoo-1, 2004]. Ve dört fazdan oluşan daha güvenilir bir yöntem önerilmiştir.

Kayıt Fazı;

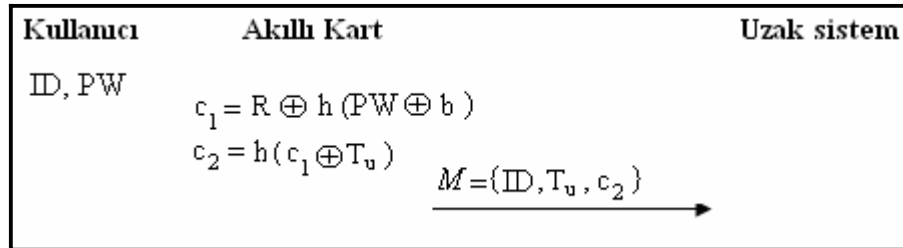
Kayıt fazında Ku-Chen yönteminden farklı olarak S de farklı bir V değeri hesaplanır. Hesaplanan bu değer $h(\cdot)$, b, R değerleriyle birlikte kayıt fazının sonunda akıllı karta yazılır (Şekil 2.8). Ve akıllı kart kullanıcıya teslim edilir.



Şekil 2.8 Yoon Ryu Yoo Yöntemi Kayıt Fazı

Bağlantı Fazı;

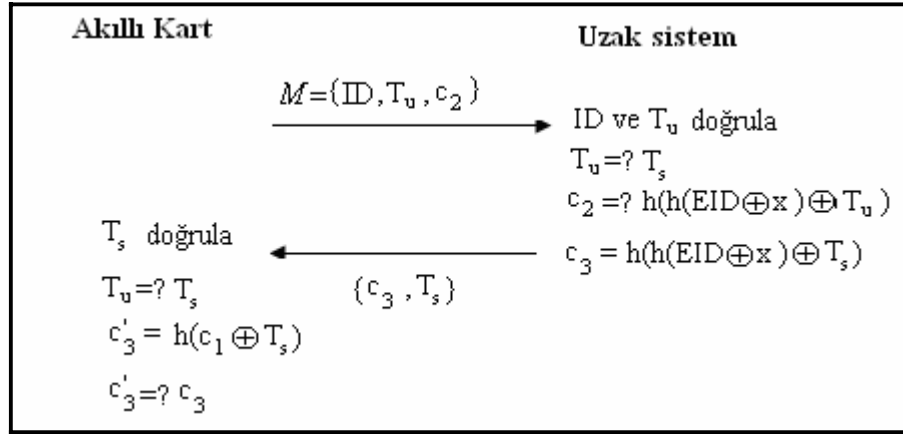
Bu faz Ku-Chen yöntemi bağlantı fazının aynısıdır. (Şekil 2.9)



Şekil 2.9 Yoon Ryu Yoo Yöntemi Bağlantı Fazı

Doğrulama Fazı;

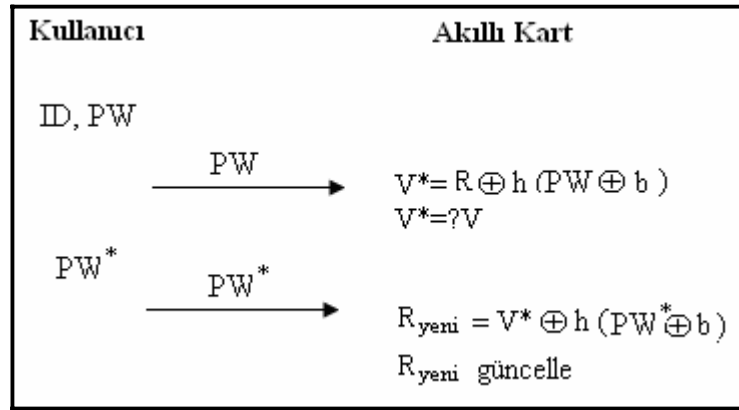
Bu fazın Ku-Chen yöntemi doğrulama fazından farkı, ID, T_u ve T_s doğrulanırken birde T_u ile T_s 'nin birbirine eşit olup olmadığı kontrolü yapılır (Şekil 2.10). Bu kontrol sayesinde paralel oturum saldırılarına karşı koruma gerçekleştirilmiş olur.



Şekil 2.10 Yoon Ryu Yoo Yöntemi Doğrulama Fazı

Şifre Değiştirme;

Bu Fazda ise Kayıt aşamasında akıllı karta yazılan V değeri yardımıyla önce girilen var olan şifrenin doğruluğu kontrolü yapılır. Daha sonra yeni şifre sisteme girilir ve ilgili değerler hesaplanır, güncellenir (Şekil 2.11).



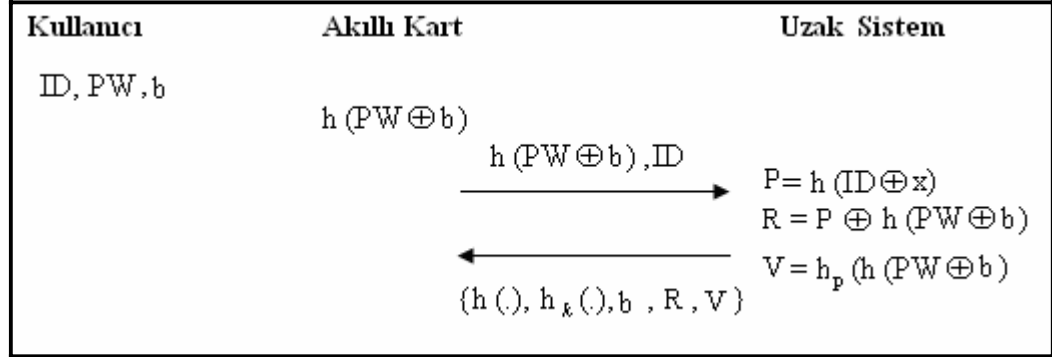
Şekil 2.11 Yoon Ryu Yoo Yöntemi Şifre Değiştirme Fazı

2.2.4 Wang Zhang Zhang Khan Yöntemi

Bu yöntemde de Wang ve diğ. Yoon ve diğ. gibi Ku-Chen yönteminin zayıflıklarını gidermek amacıyla yeni bir yöntem önermişlerdir [Wang ve diğ., 2006]. Önerilen yeni yöntem dört fazdan oluşmaktadır: Kayıt, Bağlantı, Doğrulama, Şifre Değiştirme.

Kayıt Fazı;

Kayıt Fazında Wang ve diğ., Ku-Chen ve Yoon ve diğ.'den farklı olarak kullanıcının sisteme kaç defa kayıt olduğunu sorgulamamıştır. Fazda, Şekil 2.12 de açıkça görüldüğü gibi Uzak sistemde P, R ve V değerleri hesaplanmıştır. Burada hesaplanan P değeri, V değerini hesaplarırken kullanılan anahtarlı özetleme fonksiyonuna anahtar olarak kullanılmıştır. Kayıt fazı sonunda kullanılan özetleme fonksiyonu ($h(.)$), anahtarlı özetleme fonksiyonu ($h_k(.)$) hesaplanan R,V değerleri akıllı karta yazılır. Ayrıca rasgele seçilen b sayısı kullanıcının ezberleme zorluğu da göz önünde bulundurularak akıllı karta yazılır.

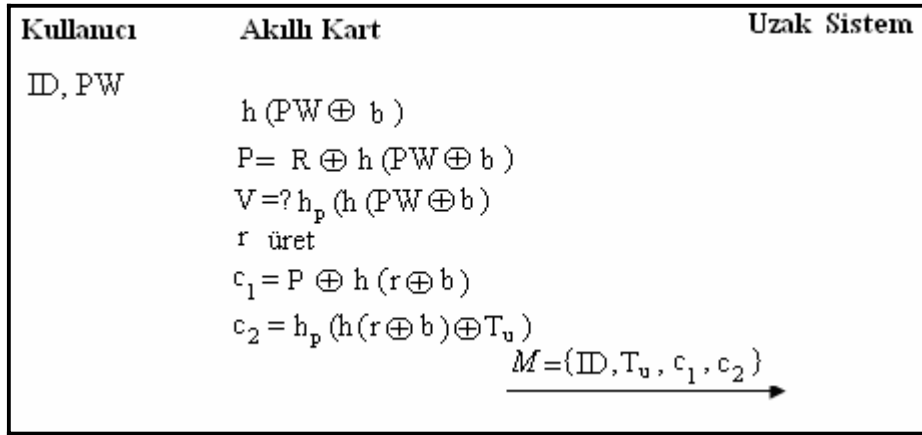


Şekil 2.12 Wang ve diğ. Yöntemi Kayıt Fazı

Bağlantı Fazı;

Bağlantı fazında, öncelikle uzak sistemin yardımı olmaksızın, kullanıcının girdiği şifrenin doğruluğu kayıt fazında akıllı karta yazılan R ve V değerleri ile test edilir. Eğer kullanıcı yanlış şifre girmiş ise bağlantı isteği reddedilir. Aksi halde akıllı kartta rasgele “r” sayısı üretilir. Üretilen r sayısı ile Şekil 2.13 de gösterildiği gibi c_1 ve c_2 değerleri

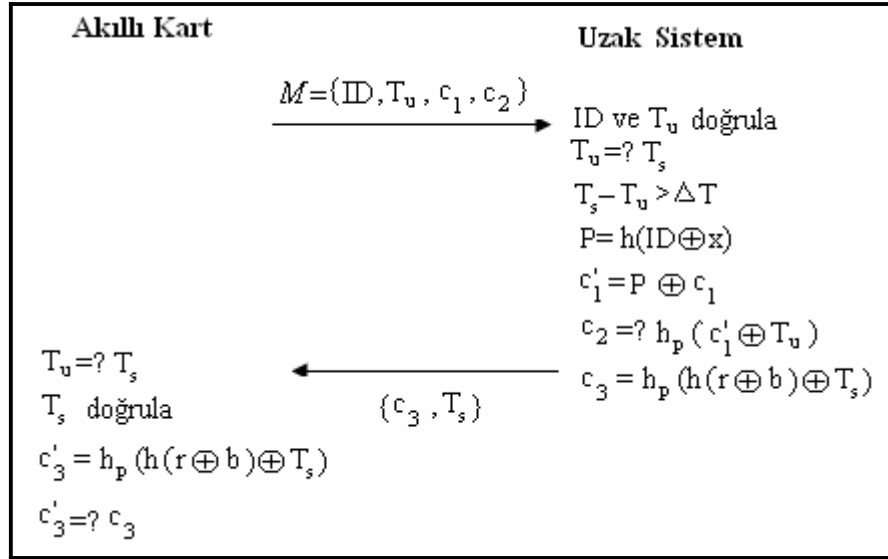
hesaplanır. Hesaplanan c_1 , c_2 kullanıcının girdiği ID ve kullanıcının o anki zamanı T_u bağlantı mesajını oluşturur ve uzak sisteme gönderilir.



Şekil 2.13 Wang ve diğ. Yöntemi Bağlantı Fazı

Doğrulama Fazı;

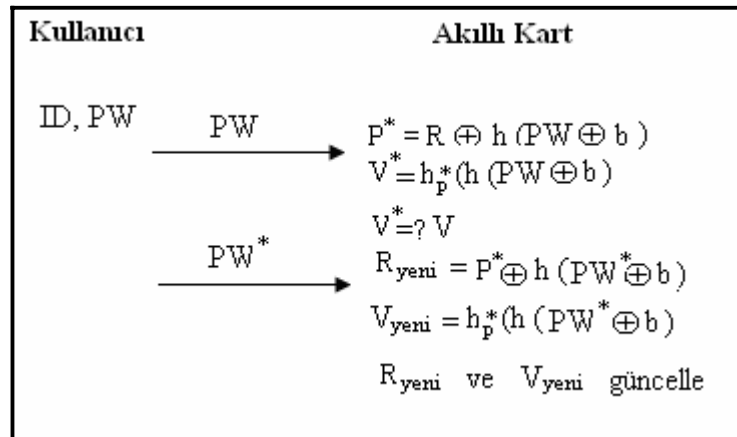
Bağlantı mesajını alan uzak sistem, önce ID ve zamanın geçerliliğini sınar ve mesajın makul bir zaman aralığında geldiğinden emin olduktan sonra, Şekil 2.14 deki gibi c_1 ve c_2 'yi hesaplar. Gönderilen c_2 değeri ile hesaplanan değer karşılaştırılır, eşitse uzak sistem kullanıcıyı doğrular. Çift taraflı doğrulama sağlamak için c_3 değeri hesaplanır ve sistemin o anki zamanıyla (T_s) birlikte akıllı kartta gönderilir. Akıllı kartta T_s 'in doğrulaması yapılır, c_3 hesaplanır, gönderilenle aynı ise çift taraflı doğrulama sağlanmış olur. Ayrıca doğrulama fazında hesaplanan c_1 ', sonraki mesajlaşmalarda oturum anahtarı olarak kullanılabilir.



Şekil 2.14 Wang ve diğ. Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Şifre değiştirme fazı Yoon ve diğ.'nın geliştirdikleri yönteminin şifre değiştirme fazıyla aynı mantıktadır. Kullanıcının şifresi uzak sisteme gitmeden akıllı kartta doğrulanır. Daha sonra yeni şifre sisteme girilir ve gerekli hesaplamalar, güncellemeler Şekil 2.15'te gösterildiği gibi yapılır.



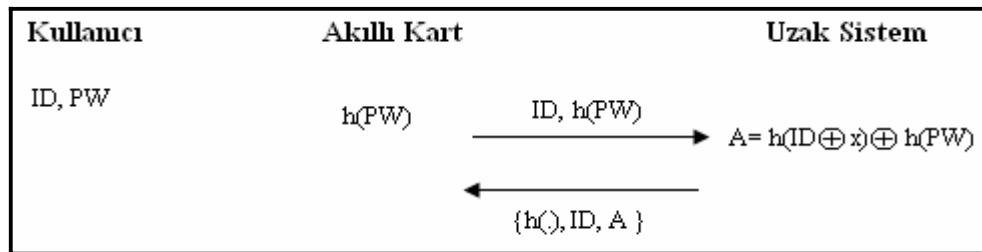
Şekil 2.15 Wang ve diğ. Yöntemi Şifre Değiştirme Fazı

2.2.5 Hwang Lee Tang Yöntemi

Yöntem Kayıt, Bağlantı, Doğrulama ve şifre değiştirme olmak üzere dört fazdan oluşur[Hwang, Lee, Tang, 2002].

Kayıt Fazı;

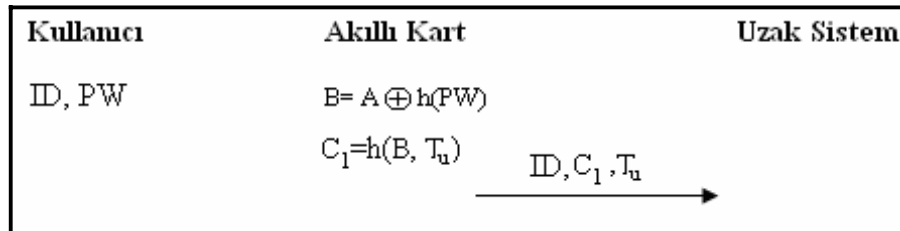
Kullanıcı sisteme seçtiği şifreyi girer. Akıllı kartta şifre özet fonksiyonuna tabi tutulur. ID ve özetlenmiş şifre uzak sisteme gönderilir. Uzak sistemde A değeri Şekil 2.16'daki gibi hesaplanır. Kullanılan özet fonksiyonu, ID ve A değerleri akıllı karta yazılır. Kayıt fazı sonunda akıllı kart kullanıcıya teslim edilir.



Şekil 2.16 Hwang Lee Tang Yöntemi Kayıt Fazı

Bağlantı Fazı;

Sisteme bağlanmak isteyen kullanıcı, akıllı kartını kart okuyucuya yerleştirir, ID ve PW ikilisini girer. Akıllı kartta Şekil 2.17'deki işlemler gerçekleştirilir. İşlemler sonunda ID, C_1 ve T_u uzak sisteme bağlantı mesajı olarak gönderilir.



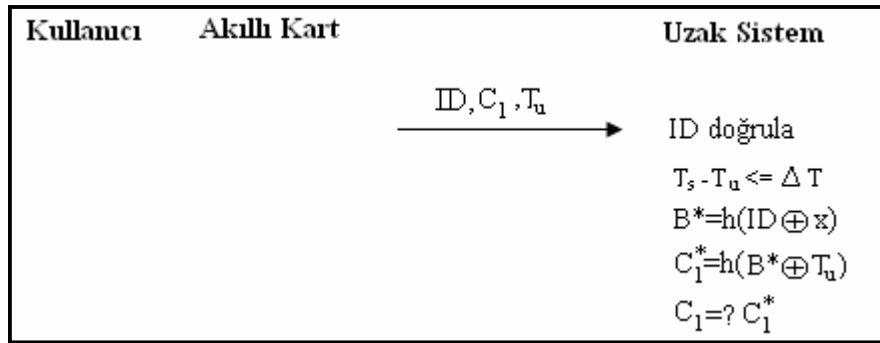
Şekil 2.17 Hwang Lee Tang Yöntemi Bağlantı Fazı

Doğrulama Fazı;

Bağlantı mesajını alan uzak sistem öncelikle (Şekil 2.18);

1. ID'nin istenilen formatta olup olmadığını kontrol eder.
2. İstenilen formatta ise mesajın gönderildiği zaman ile ulaştığı zaman farkının kabul edilebilirliğini sınar.
3. Eğer kabul edilebilirse şekildeki gibi B^* ve C_1^* değerlerini hesaplar. Hesaplanan C_1^* ile gönderilen C_1 değeri aynı ise uzak sistem kullanıcıyı doğrulamış olur.

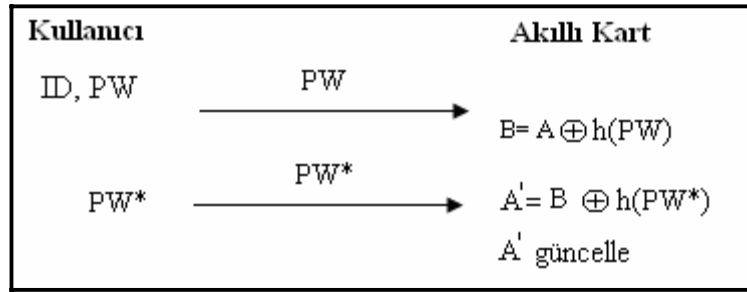
Bu yöntemde, doğrulama fazı sonunda tek taraflı doğrulama sağlanmıştır; kullanıcı uzak sistemi doğrulamamıştır.



Şekil 2.18 Hwang Lee Tang Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Kullanıcı şifresini değiştirmek istediğinde uzaktaki sisteme bağlanmadan akıllı kartta işlem gerçekleştirilir. Kullanıcı akıllı kartını yerleştirdikten sonra ID ve PW girer ve B değeri hesaplanır. Yeni PW^* girilir ve hesaplanan B değeri ile Şekil 2.19 daki gibi A' değeri hesaplanır. Akıllı karttaki A ile hesaplanan A' yer değiştirilir. Böylece kullanıcı şifresini değiştirmiş olur.



Şekil 2.19 Hwang Lee Tang Yöntemi Şifre Değiştirme Fazı

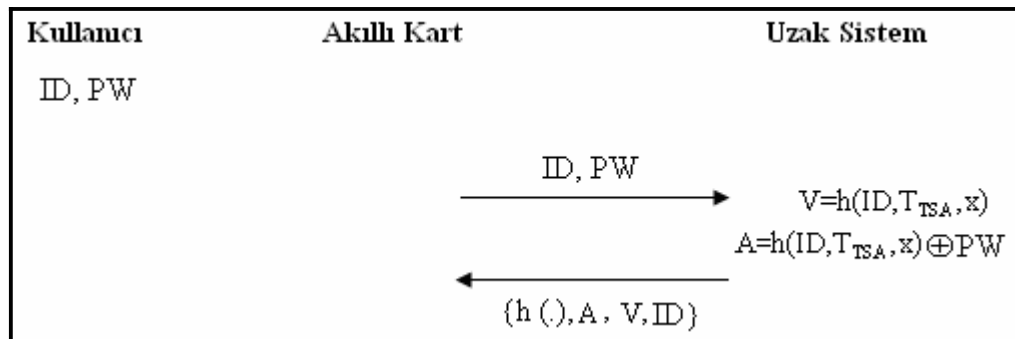
2.2.6 Yoon Ryu Yoo-2 Yöntemi

Yoon-2 ve diğ. Hwang ve diğ.'nin geliştirdikleri yönteminin zayıflıklarını gidererek yeni bir yöntem önermişlerdir [Yoon,Ryu & Yoo-2, 2004]. Bu yöntem 4 fazdan oluşur: Kayıt, Bağlantı-Doğrulama ve Şifre değiştirme.

Kayıt Fazı;

Her kullanıcı için yalnızca bir kez gerçekleşen faz şu şekildedir; Kullanıcı PW seçer ve ID ile birlikte güvenli bir kanaldan uzak sisteme iletir. Uzak sistemde V ve A değerleri hesaplandıktan sonra ID, V, h(.) ve A değerleri akıllı karta yazılır.

Yöntemde kullanılan TSA, Zaman Mührü Otoritesidir, istenildiği anda anki zamanı sağlar. Buradaki T_{TSA} Zaman mührü otoritesi tarafından sağlanan o anki zamanı temsil eder. Kayıt fazı Şekil 2.20 de özetlenmiştir.



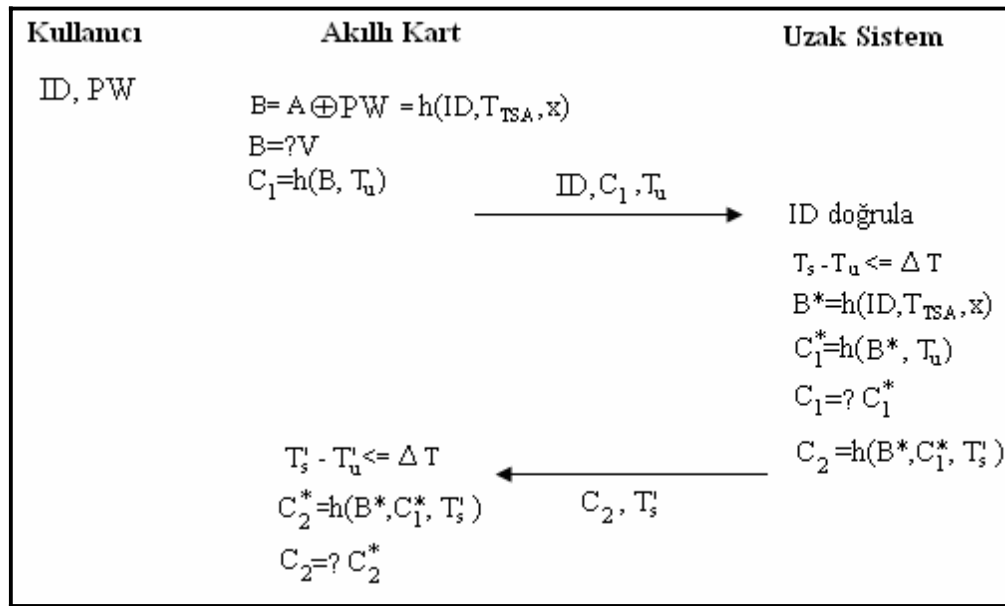
Şekil 2.20 Yoon Ryu Yoo-2 Yöntemi Kayıt Fazı

Bağlantı Fazı;

Kullanıcı uzak sisteme bağlanmak istediğinde akıllı kartını kart okuyucuya yerleştirir ve PW ile ID yi tuşlar. Akıllı kartta B hesaplanır. Hesaplanan B ile daha önceden akıllı karta kaydedilmiş V değeri karşılaştırılır eğer aynı ise C_1 hesaplanır. C_1 , T_u ve ID uzak sisteme gönderilmesiyle bağlantı fazı sona erer. Şekil 2.21’de Bağlantı ve Doğrulama fazı birlikte gösterilmektedir.

Doğrulama Fazı;

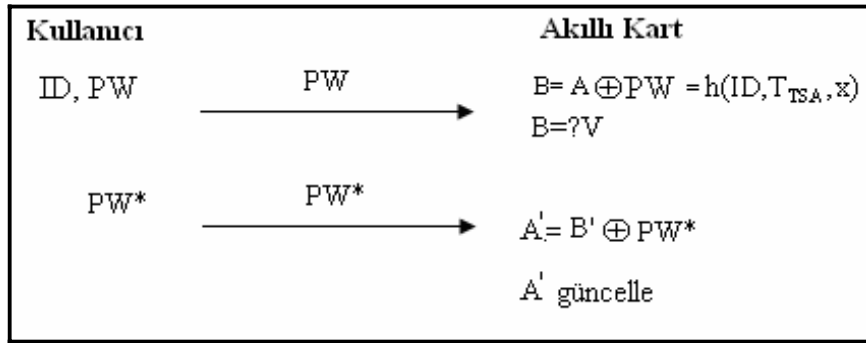
Bağlantı mesajını alan uzak sistem, önce gönderilen ID nin istenilen formatta olup olmadığını kontrol eder, istenen formatta ise zamanın makul aralıkta olup olmadığını kontrol eder. Eğer zaman da uygun ise B^* ve C_1^* hesaplanır; Hesaplanan C_1^* ile gönderilen C_1 eşit ise uzak sistem kullanıcıyı doğrulamış olur. Kullanıcının da uzak sistemi doğrulaması için C_2 hesaplanır. Buradaki T_s ’ uzak sistemin o anki zamanını temsil eder. C_2 ve T_s ’ akıllı karta gönderilir. Burada da önce zaman kontrol edildikten sonra C_2^* hesaplanır. Eğer hesaplanan değer ile gönderilen değer aynı ise kullanıcı da uzak sistemi doğrular ve böylece çift taraflı doğrulama gerçekleşmiş olur (Mutual Authentication). (Şekil 2.21)



Şekil 2.21 Yoon Ryu Yoo-2 Yöntemi Bağlantı-Doğrulama Fazı

Şifre Değiştirme Fazı;

Kullanıcı şifresini değiştirmek istediğinde uzaktaki sisteme bağlanmadan akıllı kartta işlem gerçekleştirilir. Kullanıcı akıllı kartını yerleştirdikten sonra PW girer ve B değeri hesaplanır. Hesaplanan B ile kayıtlı V değeri karşılaştırılır eşit ise kullanıcı PW değiştirme hakkına sahiptir. Yeni PW* girilir. A' değeri hesaplanır. Akıllı karttaki A ile hesaplanan A' yer değiştirilir. Böylece kullanıcı şifresini değiştirmiş olur (Şekil 2.22).



Şekil 2.22 Yoon Ryu Yoo-2 Yöntemi Şifre Değiştirme Fazı

2.2.7 Liaw Lin Wu Yöntemi

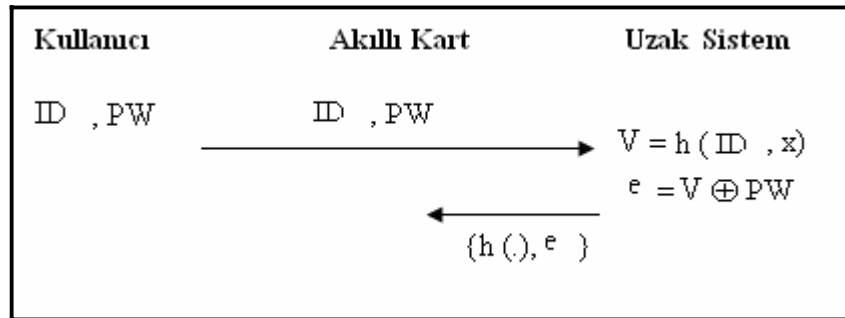
Liaw ve diğ., akıllı kart kullanarak uzaktan kimlik doğrulama yöntemi önermişlerdir[Liaw, Lin & Wu, 2006]. Bu yönteminin güvenliği tek kullanımlık sayı ve tek yönlü hash fonksiyonuna bağlıdır. Tek kullanımlık sayı değeri rasgele üretilmiş ve daha önce kullanılmamış bir değerdir ki Tekrarlı gönderme saldırılarını ve zaman senkronizasyonu problemlerini önlemek amaçlıdır.

Liaw ve arkadaşlarının önerdikleri yöntem: Kayıt Fazı, Bağlantı Fazı, Doğrulama Fazı, Oturum Fazı ve Şifre Değiştirme Fazı olmak üzere beş fazdan oluşmaktadır.

Kayıt Fazı;

Kayıt fazı, yeni bir kullanıcı sisteme katılmak istediği zaman ve her kullanıcı için sadece bir kez gerçekleşir. Fazın tamamen güvenli bir ortamda gerçekleştirildiği varsayılmaktadır. Genel olarak faz; kullanıcının, PW seçmesi ve verilen ID ile birlikte sisteme girmesi ile başlar. Sistemde V hesaplanır; Hesaplanan V değeri ile iletilen PW

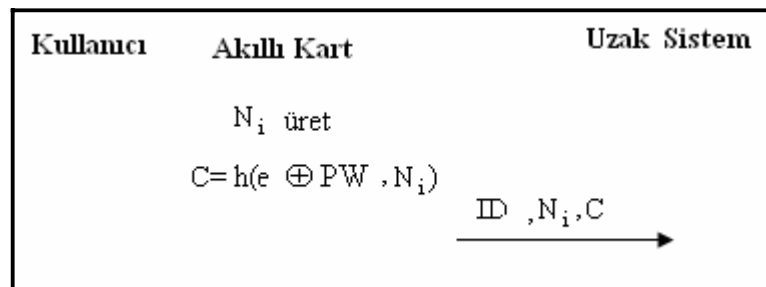
değeri mantıksal harici veya işlemine tabi tutulur(XOR) ve e elde edilir. Elde edilen e ve özetleme fonksiyonu akıllı karta yazılır. Kayıt fazı Şekil 2.23’de özetlenmiştir.



Şekil 2.23 Liaw Lin Wu Yöntemi Kayıt Fazı

Bağlantı Fazı;

Kullanıcı uzak sisteme her bağlanmak istediğinde bu faz gerçekleşir. Kullanıcı önce akıllı kartını kart okuyucuya takar ve kayıt fazında belirlenen ID ve PW girer. Daha sonra akıllı kartta bir tek kullanımlık sayı değeri N_i üretilir. İkinci adım olarak akıllı kartta bulunan e değeri ve girilen PW, XOR işlemine tabi tutulur, üretilen N_i ile birlikte özetlenerek C değeri oluşturulur, ID, N_i ve C değerleri uzak sisteme gönderilir (Şekil 2.24).



Şekil 2.24 Liaw Lin Wu Yöntemi Bağlantı Fazı

Doğrulama Fazı;

Bu faz bağlantı fazının devamıdır, bağlantı fazında uzak sisteme gönderilen mesaj bu fazda değerlendirilir. Bu fazın sonunda kullanıcı ve uzak sistem birbirlerini doğrulamış olur. Uzak sistemde sırasıyla

1. ID’nin istenilen formatta ve geçerli olup olmadığı kontrolü yapılır.

2. V' ve C değerleri hesaplanır, hesaplanan C ile gönderilen C 'nin birbirine eşitliği kontrol edilir, değilse bağlantı reddedilir.

3. Eşitse uzak sistemde sunumcu tarafında rasgele bir tek kullanımlık sayı değeri N_s üretilir.

4. Tek kullanımlık sayı değerleri şifrelenerek akıllı karta gönderilir.
 $M = E_v(N_i, N_s)$

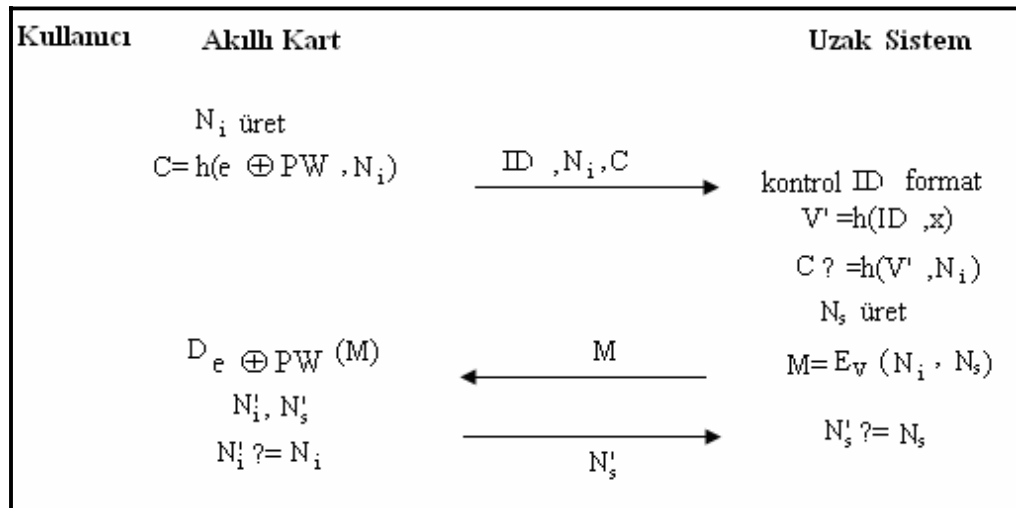
Akıllı kartta sırasıyla

1. Alınan şifreli mesaj M deşifrelenir (2.8) ve N_s' , N_i' elde edilir. N_i' ile kullanıcının N_i değerlerinin eşitliği kontrol edilir. Eşit ise kullanıcı uzak sistemi doğrulamış olur aksi durumda doğrulama işlemi reddedilir. Elde edilen N_s' uzak sisteme gönderilir.

$$D_{e \oplus PW}(M) \quad (2.8)$$

2. Alınan N_s' ile N_s eşitliği kontrol edilir. Eşitse uzak sistemde kullanıcıyı doğrulamış olur, değilse uzaktan kimlik doğrulama isteği reddedilir.

İşlemleri gerçekleştirilir. Bu işlemler bağlantı fazı da dahil olmak üzere Şekil 2.25'te gösterilmiştir.



Şekil 2.25 Liaw Lin Wu Yöntemi Doğrulama Fazı

Oturum Fazı;

Bir uzaktan kimlik doğrulama yönteminin doğrulama fazında oturum anahtarının üretilmesi önemli bir özelliktir. Üretilen oturum anahtarı doğrulama sağlandıktan sonra uzak sistem ile kullanıcı arasındaki mesajlaşmaları şifrelemek amacıyla kullanılmaktadır. Liaw yönteminde, oturum anahtarı, Diffie Helman anahtar değişim protokolü esas alınarak üretilmiştir. Burada iki açık parametre q ve α kullanılmıştır ki q büyük bir asal sayı, α ise modüler q da tanımlı primitif elemandır. Ayrıca doğrulama fazında üretilen N_s ve N_i değerlerini oturum fazında gizli anahtar olarak kullanılmıştır. Oturum fazında (Şekil 2.26) sırasıyla;

Uzak sistem $S_i = \alpha^{N_i} \text{ mod } q$ hesaplar ve akıllı karta gönderir.

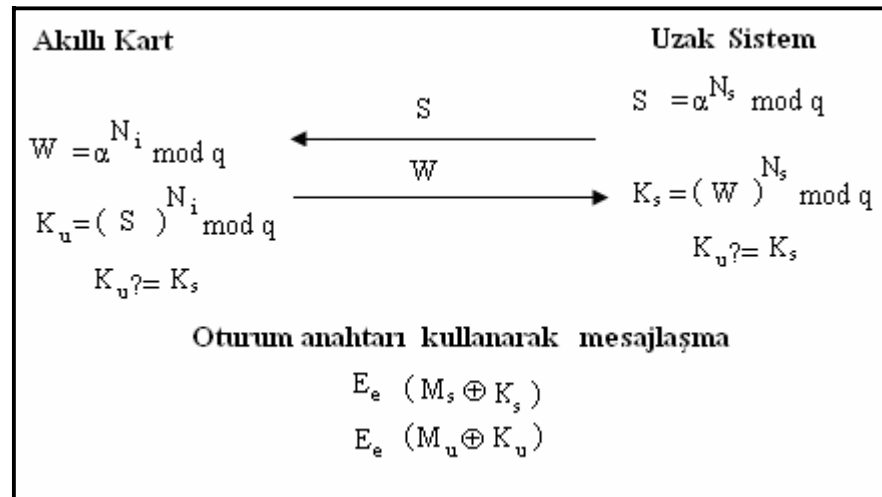
1. Akıllı kart W_i hesaplar ve uzak sisteme gönderir.
2. Uzak sistem; K_s , akıllı kart ise K_u değerlerini hesaplar. Ve her ikisi de $K_s = K_u$ eşitliğini kontrol eder. Eğer eşitse yeni bir oturum açılmıştır.

Uzak sistem kullanıcıya mesaj M_s göndermek istediğinde mesajı şifreler (2.9) ve gönderir. Kullanıcı mesajı deşifreler, K_s ile XOR operasyonuna tabi tutar ve mesajı elde eder.

$$E_e(M_s \oplus K_s) \quad (2.9)$$

3. Benzer şekilde kullanıcı uzak sisteme mesaj M_u göndermek istediğinde mesajı şifreler ve gönderir(2.10). Uzak sistem mesajı deşifreler ve K_u ile XOR operasyonuna tabi tutarak ve M_u elde eder.

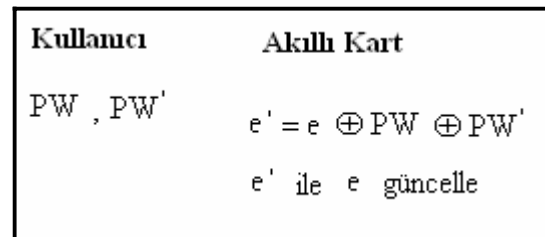
$$E_e(M_u \oplus K_u) \quad (2.10)$$



Şekil 2.26 Liaw Lin Wu Yöntemi Oturum Fazı

Şifre Değiştirme Fazı;

Liaw ve arkadaşlarının önerdikleri yöntem kullanıcının kayıt fazında belirlediği şifresini değiştirme imkanı verir. Kullanıcı değiştirmek istediği şifresini PW ve yeni şifresini PW' girer ve akıllı kartta e' hesaplaması yapılır, var olan e ile hesaplanan e' yer değiştirir. Böylece kullanıcının şifresi değişmiş olur (Şekil 2.27).



Şekil 2.27 Liaw Lin Wu Yöntemi Şifre Değiştirme Fazı

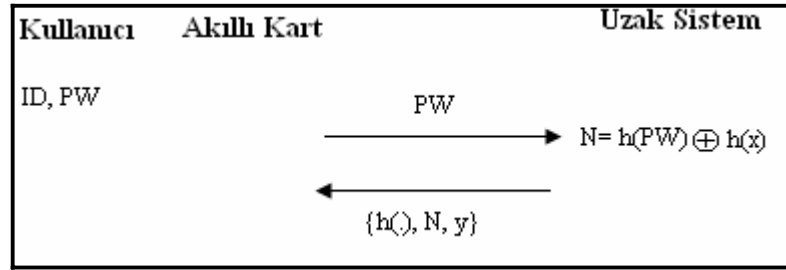
2.2.8 Das Saxena Gulati Yöntemi

Dinamik ID tabanlı yöntem [Das, Saxena, Gulati, 2004] 4 fazdan oluşur; Kayıt, Bağlantı, Doğrulama ve Şifre değiştirme.

Kayıt Fazı;

Kullanıcı ID ve PW ikilisini tuşlar. Girilen şifre uzak sisteme güvenli bir kanaldan iletilir. Uzak sistemde N şu şekilde hesaplanır; özetlenmiş PW ile özetlenmiş S'nin gizli

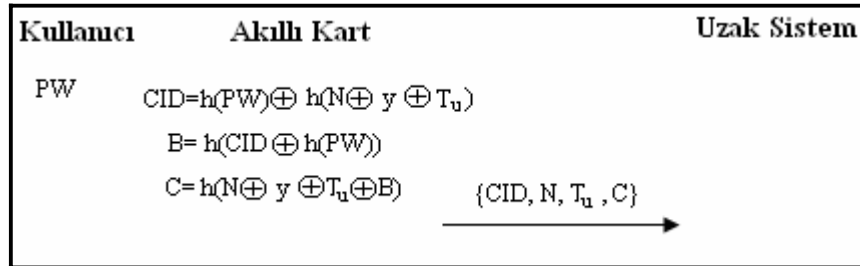
sayısı mantıksal harici veya işlemine tabi tutulur(XOR). Hesaplanan N, özetleme fonksiyonu ve y gizli sayısı akıllı karta yazılır. Kayıt fazı Şekil 2.28’de özetlenmiştir.



Şekil 2.28 Das Saxena Gulati Yöntemi Kayıt Fazı

Bağlantı Fazı;

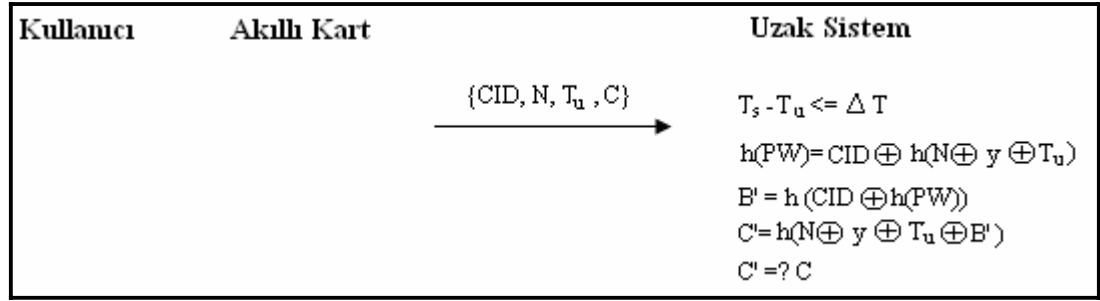
Bu faz kullanıcı sisteme her bağlanmak istediğinde gerçekleşir. Bağlantı kullanıcının akıllı kartını kart okuyucuya yerleştirerek PW ve ID girmesi ile başlar. Daha sonra akıllı kart dinamik ID’yi (CID) hesaplar. Sonra ki adımda B ve C hesaplanır. Hesaplanan CID, C ve akıllı karta yazılmış olan N ile kullanıcının o anki zaman mührü (T_u) uzak sisteme gönderilir.



Şekil 2.29 Das Saxena Gulati Yöntemi Bağlantı Fazı

Doğrulama Fazı;

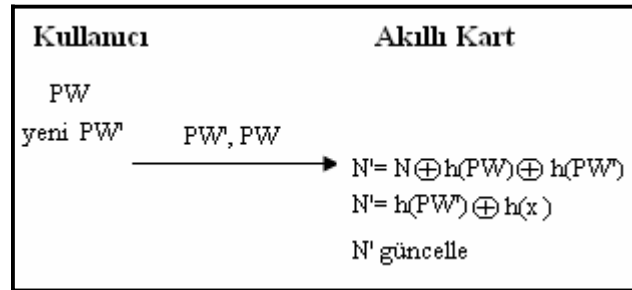
Bağlantı isteği mesajını alan uzak sistem, önce T_u kontrolünü yapar, mesaj makul zaman aralığında ulaşmış ise $h(PW)$ ’ü hesaplar. Daha sonra elde ettiği $h(PW)$ ile B’ ve C’ değerlerini hesaplar. Hesaplanan C’ ile kullanıcıdan gelen C değerleri kontrol edilir. Eğer eşitse doğrulama biter, değilse kullanıcı reddedilir. Faz sona erdiğinde tek taraflı doğrulama gerçekleşmiş olur. Doğrulama fazı Şekil 2.30 da gösterilmiştir.



Şekil 2.30 Das Saxena Gulati Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Kullanıcı akıllı kartını kart okuyucuya yerleştirir ve PW girer kullanıcı uzak sistem tarafından doğrulanmadan şifresini değiştirme isteğinde bulunur ve yeni PW' girer. Akıllı kartta N' hesaplanır, hafızadaki N ile N' yer değiştirilerek şifre değiştirilmiş olur. Şifre değiştirme fazı Şekil 2.31'de özetlenmiştir.



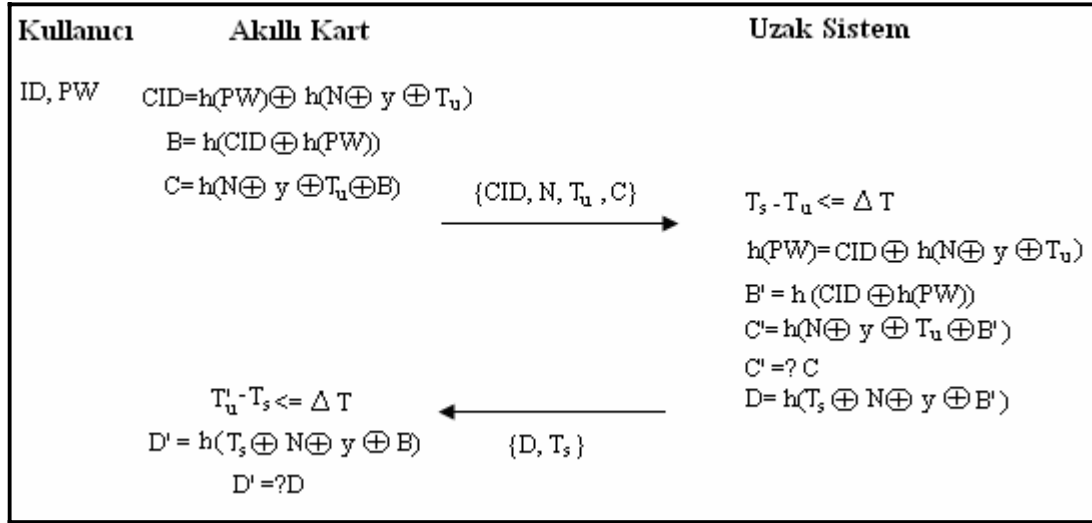
Şekil 2.31 Das Saxena Gulati Yöntemi Şifre Değiştirme Fazı

2.2.9 Liao Lee Hwang Yöntemi

Liao ve diğ., 2004 yılında Das, Saxena ve Gulatinin (DSG) geliştirmiş oldukları dinamik ID tabanlı, uzaktan kimlik doğrulama yönteminin noksan yönlerini geliştirerek yeni yöntem oluşturmuşlardır [Liao, Lee, Hwang, 2005]. Bu yeni yöntem üç fazdan oluşmaktadır; Kayıt fazı ve Doğrulama fazı. Ayrıca kullanıcıya şifre değiştirme imkânının verildiği Şifre değiştirme fazı.

Kayıt Fazı;

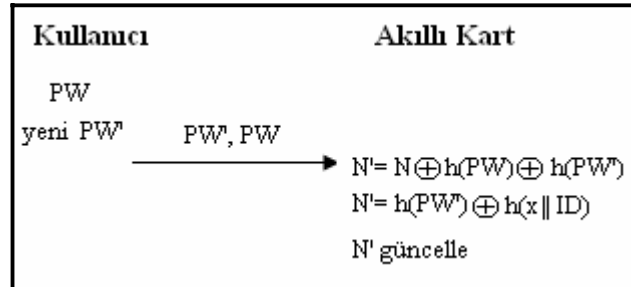
Kullanıcı, ID sini girer ve PW seçer. Akıllı kartta PW özetleme fonksiyonuna tabi tutulur. ID ve h(PW) güvenli bir kanaldan uzak sisteme ulaştırılır. Uzak sistemde N



Şekil 2.33 Liao Lee Hwang Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Liao ve arkadaşları, Das, Saxena ve Gulati yönteminin şifre değiştirme fazını aynen almış değiştirmeye ihtiyaç duymamışlardır. Kullanıcı akıllı kartını kart okuyucuya yerleştirir ve PW girer kullanıcı uzak sistem tarafından doğrulanmadan şifresini değiştirme isteğinde bulunur ve yeni PW' girer. Akıllı kartta N' hesaplanır, hafızadaki N ile N' yer değiştirilerek şifre değiştirilmiş olur. Şifre değiştirme fazı Şekil 2.34'te özetlenmiştir.



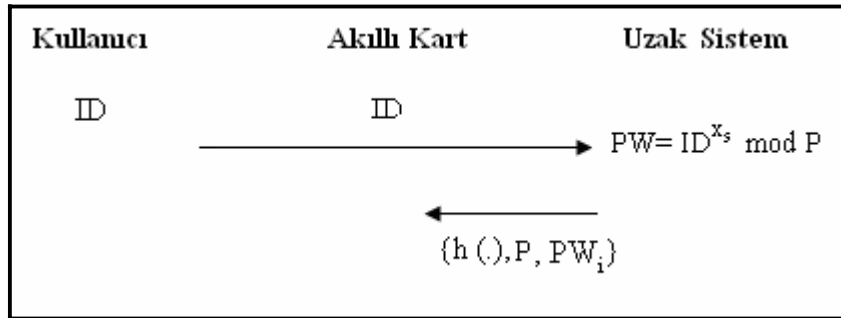
Şekil 2.34 Liao Lee Hwang Yöntemi Şifre Değiştirme Fazı

2.2.10 Hwang Li Yöntemi

Bu yöntem[Hwang, Li, 1999] üç ana fazdan oluşur Kayıt, Bağlantı ve Doğrulama. Şifre kayıt esnasında bir kere hesaplanır ve değiştirilemez. Dolayısıyla şifre değiştirme fazı yoktur.

Kayıt Fazı;

Diğer yöntemlerden farklı olarak burada kullanıcı şifresini girmez, kullanıcının ID değerine göre şifre uzak sistemde hesaplanır. Hesaplanan şifre, hash fonksiyonu ve modüler işlemde kullanılan 1024 bit büyük asal sayı olan P akıllı karta yazılır. Kayıt fazı Şekil 2.35'te özetlenmiştir.

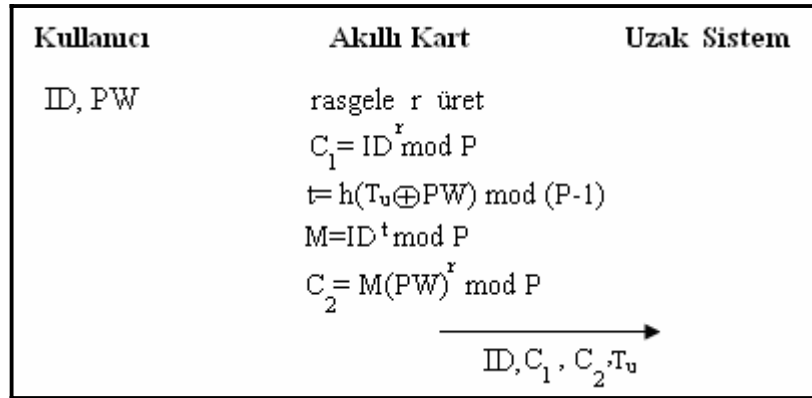


Şekil 2.35 Hwang Li Yöntemi Kayıt Fazı

Bağlantı Fazı;

Bağlantı fazında kullanıcı, kayıt fazında sistem tarafından hesaplanan şifreyi ve ID sini sisteme girer. Sonra akıllı kart sırasıyla aşağıdaki işlemleri gerçekleştirir (Şekil 2.36);

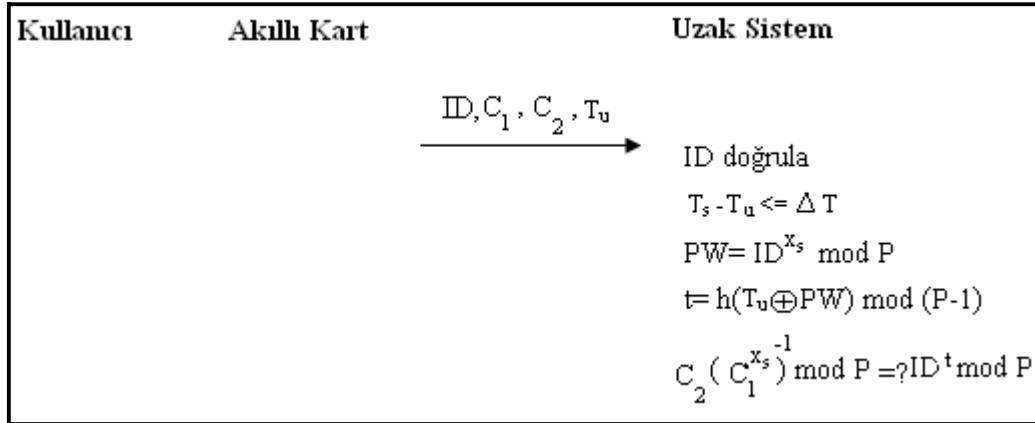
1. Rasgele r sayısı üretilir.
2. Üretilen r sayısı ile şekildeki gibi C_1 hesaplanır.
3. Daha sonra sırasıyla t, M ve C_2 değerleri hesaplanır.
4. ID, C_1 , C_2 , T_u uzak sisteme bağlantı mesajı olarak gönderilir.



Şekil 2.36 Hwang Li Yöntemi Bağlantı Fazı

Doğrulama Fazı;

Bağlantı mesajını alan uzak sistem, önce gönderilen ID nin istenilen formatta olup olmadığını kontrol eder, istenen formatta ise zamanın makul aralıkta olup olmadığını kontrol eder. Eğer zaman da uygun ise PW ve t hesaplanır; Gönderilen C_1 ile C_2 değerleriyle hesaplanan değer, hesaplanan t değeriyle elde edilen M değerine eşit ise uzak sistem kullanıcıyı doğrulamış olur. Doğrulama fazı sonunda tek taraflı doğrulama gerçekleştirilmiş olur.(Şekil 2.37)



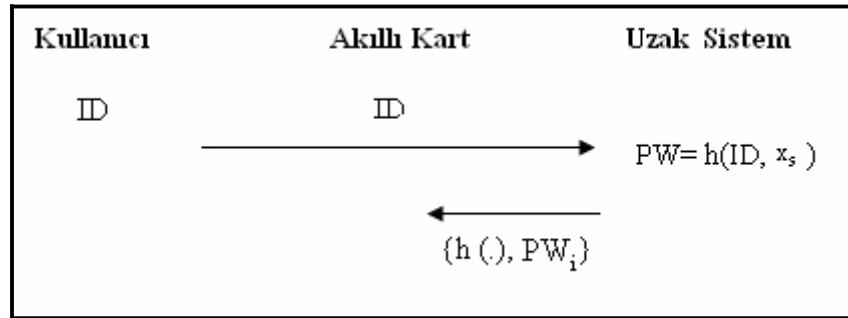
Şekil 2.37 Hwang Li Yöntemi Doğrulama Fazı

2.2.11 Sun Yöntemi

Sun tarafından önerilen bu yöntem Hwang- Li yönteminin eksikliklerinden yola çıkılarak önerilmiştir [Sun,2000]; üç ana fazdan oluşur Kayıt, Bağlantı ve Doğrulama. Şifre kayıt esnasında bir kere hesaplanır ve değiştirilemez. Dolayısıyla şifre değiştirme fazı yoktur.

Kayıt Fazı;

Hwang-Li yöntemindeki gibi burada da kullanıcı şifresini girmez, kullanıcının ID değerine göre şifre uzak sistemde hesaplanır. Hesaplanan şifre karta yazılır. Kayıt fazı Şekil 2.38’de özetlenmiştir.

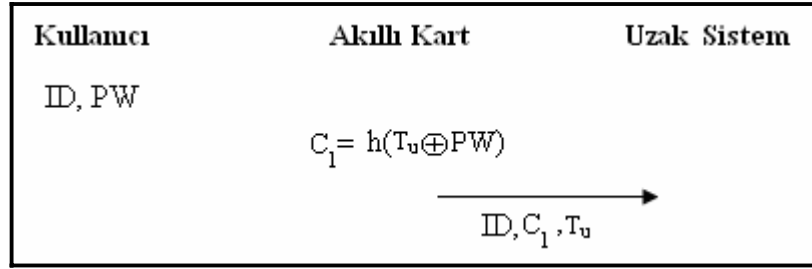


Şekil 2.38 Sun Yöntemi Kayıt Fazı

Bağlantı Fazı;

Bağlantı fazında kullanıcı, kayıt fazında sistem tarafından hesaplanan şifreyi ve ID sini sisteme girer. Sonra akıllı kart sırasıyla aşağıdaki işlemleri gerçekleştirir (Şekil 2.39);

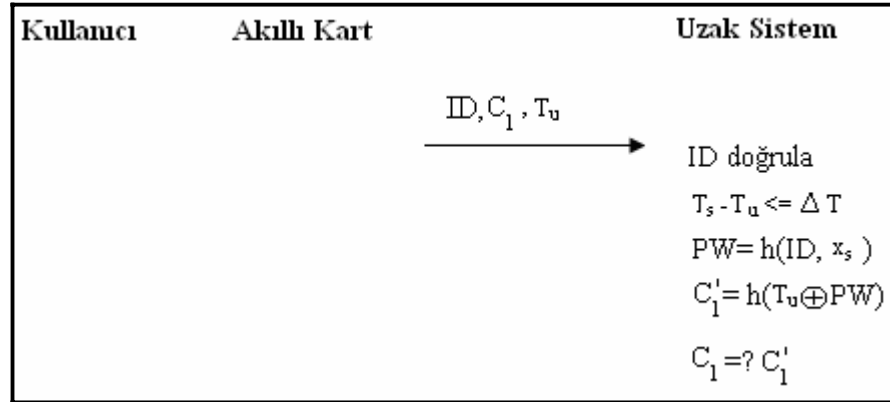
1. Girilen şifre ve kullanıcın o anki zamanı ile C_1 hesaplanır.
2. ID, C_1 , T_u uzak sisteme bağlantı mesajı olarak gönderilir.



Şekil 2.39 Sun Yöntemi Bağlantı Fazı

Doğrulama Fazı;

Bağlantı mesajını alan uzak sistem, önce gönderilen ID'nin istenilen formatta olup olmadığını kontrol eder, istenen formatta ise zamanın makul aralıkta olup olmadığını kontrol eder. Eğer zaman da uygun ise PW ve C_1' hesaplanır; Gönderilen C_1 ile C_1' eşit ise uzak sistem kullanıcıyı doğrulamış olur. Doğrulama fazı sonunda tek taraflı doğrulama gerçekleştirilmiş olur (Şekil 2.40).



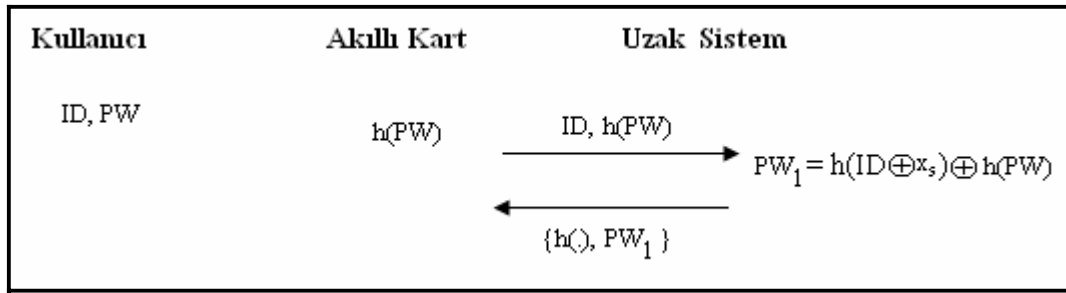
Şekil 2.40 Sun Yöntemi Doğrulama Fazı

2.2.12 Lee Hwang Yang Yöntemi

Lee ve diğ. tarafından önerilen bu yöntem de Sun yönteminin eksikliklerinden yola çıkılarak önerilmiştir[Lee, Hwang & Yang, 2005]; dört ana fazdan oluşur Kayıt, Bağlantı ve Doğrulama ve Şifre değiştirme fazı.

Kayıt Fazı;

Sun yönteminden farklı olarak burada kullanıcı bir şifre seçer. Akıllı kartta özetlenen şifre ID ile birlikte güvenli kanaldan uzak sisteme iletilir. Uzak sistemde ikinci bir PW_1 hesaplanır. Hesaplanan şifre PW_1 ve özetleme fonksiyonu karta yazılır. Kayıt fazı Şekil 2.41’de özetlenmiştir.

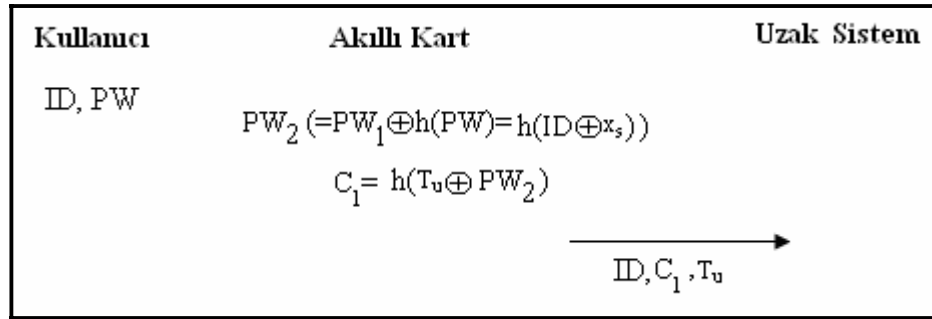


Şekil 2.41 Lee Hwang Yang Yöntemi Kayıt Fazı

Bağlantı Fazı;

Bağlantı fazında kullanıcı, PW ve ID sini sisteme girer. Sonra akıllı kart sırasıyla aşağıdaki işlemleri gerçekleştirir (Şekil 2.42);

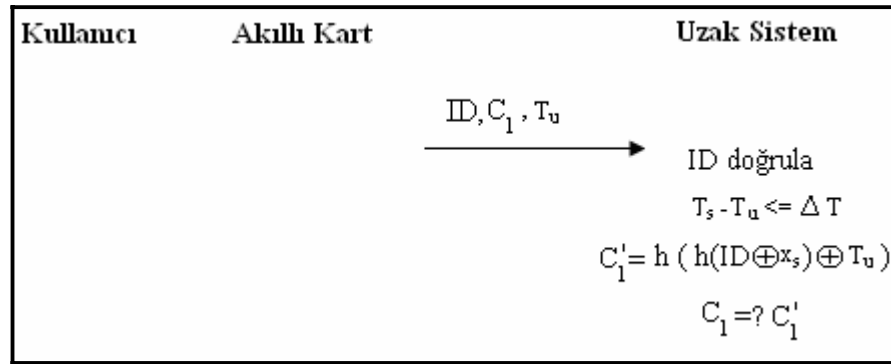
1. PW_2 , ve C_1 hesaplanır.
2. ID, C_1 , T_u uzak sisteme bağlantı mesajı olarak gönderilir.



Şekil 2.42 Lee Hwang Yang Yöntemi Bağlantı Fazı

Doğrulama Fazı;

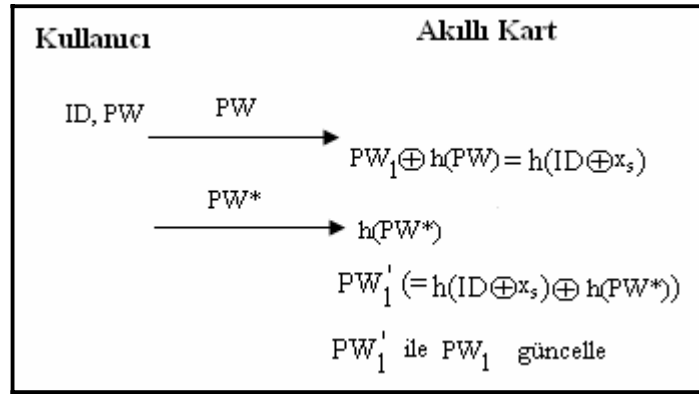
Bağlantı mesajını alan uzak sistem, önce gönderilen ID nin istenilen formatta olup olmadığını kontrol eder, istenen formatta ise zamanın makul aralıkta olup olmadığını kontrol eder. Eğer zaman da uygun ise C_1' hesaplanır; Gönderilen C_1 ile C_1' eşit ise uzak sistem kullanıcıyı doğrulamış olur. Doğrulama fazı sonunda tek taraflı doğrulama gerçekleştirilmiş olur.(Şekil 2.43)



Şekil 2.43 Lee Hwang Yang Yöntemi Doğrulama Fazı

Şifre Değiştirme Fazı;

Sun yönteminde olmayan bu faz kullanıcıya şifre değiştirme olanağı sağlar. Kullanıcı akıllı kartını kart okuyucuya yerleştirir, ID ve PW girer kullanıcı uzak sistem tarafından doğrulanmadan şifresini değiştirme isteğinde bulunur ve yeni PW^* girer. Akıllı kartta PW_1' hesaplanır, hafızadaki PW_1 ile PW_1' yer değiştirilerek şifre değiştirilmiş olur. Şifre değiştirme fazı Şekil 2.44'te özetlenmiştir.



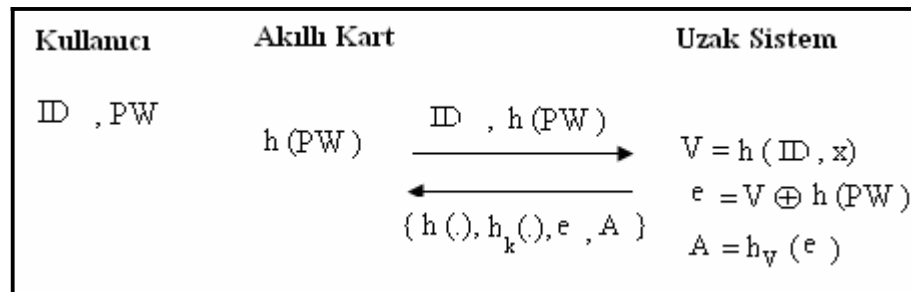
Şekil 2.44 Lee Hwang Yang Yöntemi Şifre Değiştirme Fazı

3. ÖNERİLEN YÖNTEM

Bu çalışmada Liaw ve diğ.’nin geliştirdikleri yöntemin eksik yönleri giderilerek oluşturulan yeni bir yöntem önerilmiştir. Bu yöntemin diğer doğrulama yöntemlerinden farkı, kullandığı kriptografik yöntemdir, daha önce kullanılan yöntemler; RSA tabanlı, El-Gamal tabanlı, özetleme fonksiyonu tabanlı iken burada eliptik eğri kriptografisi ve özet fonksiyonu tabanlı sistem kombine edilerek yeni yönteme uygulanmıştır. Bu yöntem üç fazdan oluşmaktadır: Kayıt fazı ve Doğrulama Fazının yanı sıra kullanıcının kayıt fazından sonra şifre değiştirmesine izin veren Şifre Değiştirme Fazı.

3.1 Kayıt Fazı

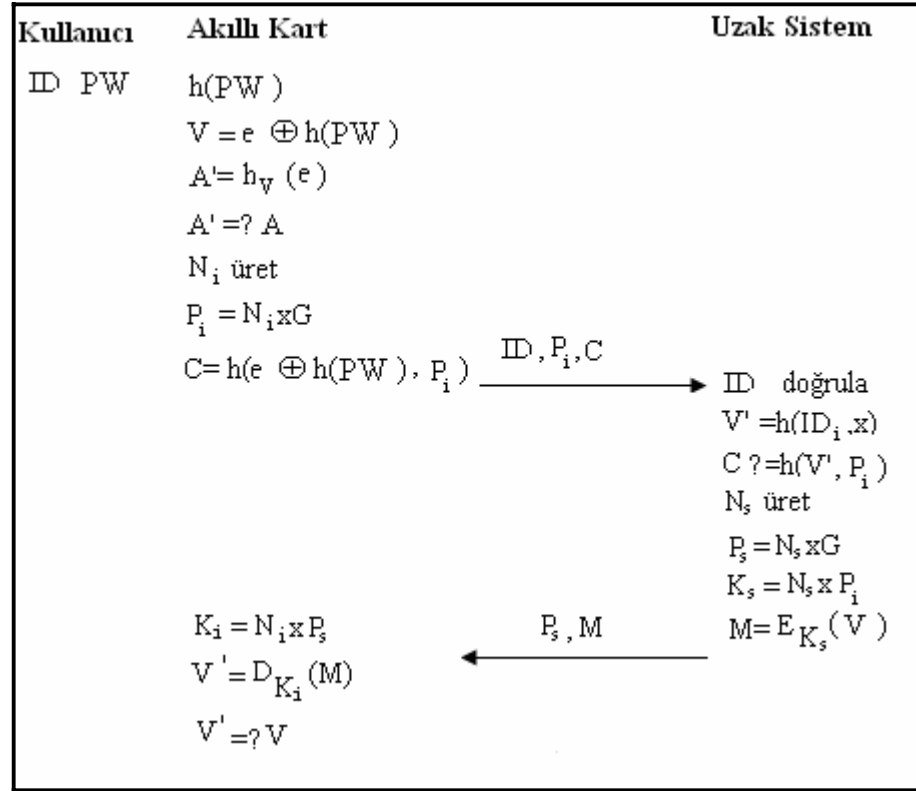
Kayıt fazı, Liaw ve diğ. yönteminin kayıt fazı temel alınarak oluşturulmuştur. Önerilen yöntemde, Liaw ve diğ. yöntemindeki girilen şifrenin düz metin olarak gönderilmesinden dolayı oluşan sıkıntı giderilmiştir. Yani akıllı kartta şifrenin özetlenmesi, sistem yöneticisi tarafından şifrenin açık olarak görülmesini engellemiştir. Liaw yönteminden bir diğer fark ise “A” değerinin hesaplanmasıdır. “A” değeri kullanıcı şifresini girdiğinde uzak sisteme gitmeden akıllı kartta şifrenin doğruluğunu kontrol etmeye yardımcı olmaktadır. Bütün yöntemlerin kayıt fazında olduğu gibi bu faz sadece yeni kullanıcı sisteme katılmak istediğinde, her kullanıcı için bir kez gerçekleşir. Şekil 3.1 de görüldüğü gibi uzak sistem tarafından V, e ve A değerleri hesaplanır. A, e, $h(.)$ ve $h_k(.)$ daha sonradan yapılacak olan hesaplamaları kontrol etmek amacıyla akıllı karta yazılır.



Şekil 3.1 Önerilen Yöntem Kayıt Fazı

3.2 Doğrulama Fazı

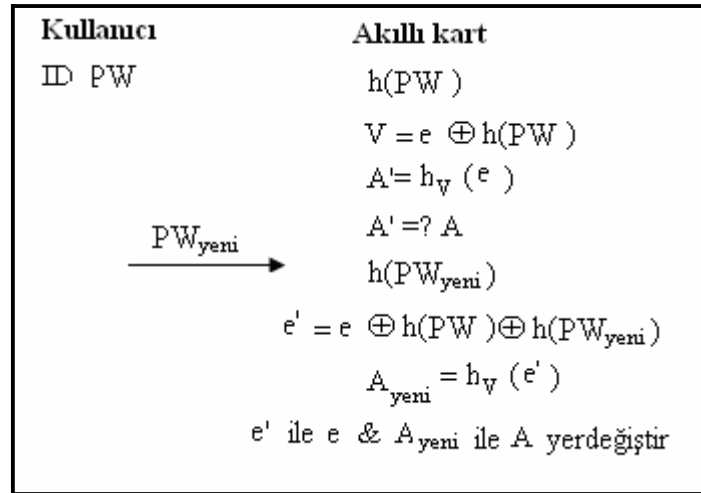
Önerilen yöntemin doğrulama fazı, diğer yöntemlerden kullandığı kriptografik yöntem açısından ayrılır. Burada Eliptik Eğri Diffie Hellman (EEDH) kriptografi temel alınmıştır. EEDH daha kısa anahtar uzunluğu olanağı vermesinden dolayı kullanılmıştır. Bölüm 2.1.4'te bahsedildiği üzere hem kullanıcı hem de uzak sistem aynı eliptik eğriyi ve bu eğri üzerindeki “G” taban noktasını daha önceden bildikleri varsayılmaktadır. EEDH 'nin sağladığı güvenlik özelliklerine ek olarak; Liaw ve diğ. yöntemindeki, tek kullanımlık sayı değeri ve hash fonksiyonunun da sağladığı güvenlik özellikleri önerilen yöntemde mevcuttur. Liaw ve diğ. yönteminden diğer bir farkta, kullanıcı PW girdiğinde uzak sisteme gitmeden akıllı kartta girilen şifrenin doğru olup olmadığı, kayıt fazında akıllı karta kaydedilen “A” değeri yardımıyla sorgulanır. Böylece yanlış PW girildiğinde tespiti kolay ve hızlı olur. Eğer PW doğruysa N_i değeri EEDH ye uygun şekilde rasgele üretilir. P_i ve C değerleri hesaplandıktan sonra ID ile birlikte uzak sisteme gönderilir. Uzak sistemde gönderilen mesajdaki değerlerin doğruluğu test edilir, doğruysa uzak sistem kullanıcıyı doğrular ve rasgele N_s değeri üretir. Üretilen N_s ile P_s ve K_s değeri hesaplanır. K_s anahtarı ile şifrelenen V değeri ile P_s akıllı karta gönderilir. Akıllı kartta K_i değeri hesaplanır ki bu değer K_s değerine eşit olmalıdır. Hesaplanan K_i ile gönderilen mesaj deşifrelenir. Gönderilen V değerinin doğruluğu sınanır eğer doğru ise kullanıcı da uzak sistemi doğrulamış olur. Böylece iki taraflı (mutual) kimlik doğrulama yapılmış olur. Doğrulama fazında üretilen K_s ve K_i değerleri, daha sonra kullanıcı ile uzak sistem iletişimde oturum anahtarı olarak kullanılır. Doğrulama fazı Şekil 3.2 de gösterilmiştir.



Şekil 3.2 Önerilen Yöntem Doğrulama Fazı

3.3 Şifre Değiştirme Fazı

Önerilen yöntemin Şifre değiştirme fazında uzak sisteme gerek kalmadan akıllı kartta değişim gerçekleşir. Bu fazın Liaw yöntemindeki şifre değiştirme fazından farkı, şifre değiştirmeden önce eski şifrenin doğruluğunun kontrol edilmesidir. Sistem, şifre tahmini saldırısını önlemek için üç kez yanlış şifre girildiğinde kart okuyucunun akıllı kartı bloke edecek şekilde tasarlanmıştır. Bu tasarım yöntemin akıllı kartın kaybolması durumunda da güvenliği sağlamasına yardımcı olur. Şifre değiştirme fazı Şekil 3.3 te gösterilmiştir.



Şekil 3.3 Önerilen Yöntem Şifre Değiştirme Fazı

4. TEST SONUÇLARI KARŞILAŞTIRMA VE GÜVENLİK ANALİZİ

Tezin bu bölümünde teorik ve pratik olarak yöntemlerin hesaplama maliyetleri karşılaştırılacaktır. Önerilen yöntem , Liaw ve diğ., Wang ve diğ. ve Liao ve diğ.’nin önerdikleri yöntemler java platformunda ve 1.60 GHz dual-core Intel Pentium 512 MB hafıza kapasiteli bilgisayarda gerçekleştirilmiştir.

Önerilen yöntem gerçekleştirirken, NIST’ in önerdiği eliptik eğri listesinden seçilen B-163 normal tabanlı eğri kullanılmıştır[NIST, 1999]. Ayrıca SHA tabanlı HMAC fonksiyonu anahtarlı özetleme fonksiyonu olarak kullanılmıştır. Eliptik eğri scalar çarpımında daha hızlı hesaplama yapabilmek için de “2P: The Montgomery Scalar Multiplication algorithm” yöntemi kullanılmıştır[Lopez ve diğ., 1999]. Ve bütün yöntemlerin benzetimi için gerekli Güvenli rasgele sayı üretici (Secure Random Generator), SHA-512 ve AES sırasıyla tek kullanımlık sayı üretme, özetleme fonksiyonu ve simetrik şifreleme amaçlarıyla java kriptografi kütüphanesinden kullanılmıştır.

4.1 Hesaplama maliyeti analizi ve benzetim sonuçları

Teorik olarak önceki bölümde bahsi geçen dört yöntemin hesaplama maliyetlerinin karşılaştırılması Çizelge 4.1 de verilmiştir. Test sonuçları ise Çizelge 4.2 de görülmektedir. Çizelge 4.2 de verilen test sonuçları, her bir bağlantı isteğinde üretilecek tek kullanımlık sayı’ya göre doğrulama işleminin alacağı zaman değişeceği için on bağlanma sonucu alınan zamanların ortalaması alınarak hesaplanmıştır. Ayrıca Akıllı karta hesaplanan değerlerin yazılması/okunması ve uzak sistem ve kullanıcı arasındaki mesajlaşmada geçen süreler ihmal edilmiştir. Ve Çizelge 4.1 de karşılaştırma sabit zaman alacağı için ihmal edilmiştir.

Çizelge 4.1 Hesaplama Maliyetlerinin Karşılaştırılması

YÖNTEM	KAYIT	BAĞLANTI	DOĞRULAMA	OTURUM	ŞİFRE DEĞİŞTİRME
Liaw ve diğ.	$1T_{(f)}$ $1T_{\oplus}$	$1T_{(f)}$ $1T_{\oplus}$ $1T_{(q)}$	$2T_{(f)}$ $1T_{(q)}$ $2T_{(SE)}$	$1T_{\oplus}$ $2T_{(ME)}$	$2T_{\oplus}$
Wang ve diğ.	$2T_{(f)}$ $1T_{(k)}$ $3T_{\oplus}$ $1T_{(q)}$	$2T_{(f)}$ $2T_{(k)}$ $5T_{\oplus}$ $1T_{(q)}$	$2T_{(f)}$ $3T_{(k)}$ $6T_{\oplus}$	-	$2T_{(f)}$ $2T_{(k)}$ $4T_{\oplus}$
Liao ve diğ.	$2T_{(f)}$ $1T_{\oplus}$	-	$9T_{(f)}$ $20T_{\oplus}$	-	$2T_{(f)}$ $2T_{\oplus}$
Önerilen	$2T_{(f)}$ $1T_{(k)}$ $1T_{\oplus}$	-	$4T_{(f)}$ $2T_{SE}$ $1T_{(k)}$ $2T_{(q)}$ $4T_{(s)}$ $1T_{\oplus}$	-	$2T_{(f)}$ $2T_{(k)}$ $2T_{\oplus}$

$T_{(f)}$: Tek yönlü özetleme fonksiyonu hesaplama maliyeti

$T_{(k)}$: Anahtarlı tek yönlü özetleme fonksiyonu hesaplama maliyeti

$T_{\oplus}$: XOR operasyonu hesaplama maliyeti

$T_{(SE)}$: Simetrik şifreleme hesaplama maliyeti

$T_{(ME)}$: Modüler üst alma hesaplama maliyeti

$T_{(q)}$: Rasgele sayı üretme hesaplama maliyeti

$T_{(s)}$: ECDH 'de skaler nokta çarpımı hesaplama maliyeti

Çizelge 4.2 Hesaplama Maliyetleri Test Sonuçları

YÖNTEM	KAYIT (msn)	BAĞLANTI (msn)	DOĞRULAMA (msn)	OTURUM (msn)	YANLIŞ ŞİFRE TESPİT (msn)
Liaw ve diğ.	16	94	826,6	1msec den az	86,1
Wang ve diğ.	32	125	15,7	-	12,6
Liao ve diğ.	23	-	15,3	-	12,3
Önerilen	31	-	912.5	-	6,1

Çizelge 4.1 ve Çizelge 4.2 de Liaw ve diğ. yönteminin oturum fazı sadece oturum anahtarının üretilmesi kısmı esas alınmıştır. Çizelgelerde verilen değerlere bu oturum anahtarını kullanarak mesajlaşma dahil değildir.

Her iki çizelgenin de birbirleri arasında tutarlı oldukları açıktır. Sadece Liaw ve diğ.'nin önerdikleri yöntemin oturum fazı Çizelge 4.1 de beklendiği gibi değil de daha hızlı olduğu test sonuçlarında görülmektedir. Bunun sebebi Java'nın kullandığı modüler üst alma fonksiyonunun zaman karmaşıklığıdır.

Ayrıca Liaw ve diğ. ile önerilen yöntemde kullanılan simetrik şifreleme her iki yöntemin doğrulama fazına diğer gerçekleştirilen yöntemlere kıyasla çok fazla ek maliyet getirir.

Gerçeklenme sonuçları önerilen yöntemin, sağladığı güvenlik özelliklerini de göz önünde bulundurularak karşılaştırılabilir hesaplama maliyeti olduğunu göstermektedir.

4.2 Önerilen Yöntemin Güvenlik Analizi

Önerilen yöntemin güvenlik analizi ve özellikleri aşağıda verilmiştir.

1. Uzak sistemde şifre veya doğrulama çizelgesi tutulmaz. Daha önce önerilen bazı yöntemlerde sunumcu tarafında doğrulama çizelgesinin tutulduğundan bahsedilmişti, n tane kullanıcı olduğu varsayılırsa; sistemin kullanıcı tanımlayıcılarını ve şifrelerini tutmak için $O(n)$ kadar yere ihtiyacı olacaktır. Fakat önerilen yöntemde yer ihtiyacı $O(1)$ olacaktır.

2. Kayıt fazında, kullanıcı kendi istediği şifreyi seçilebilmekte ve istediği takdirde kolaylıkla değiştirilebilmektedir. Sunumcu şifrenin seçilmesine ve değiştirilmesine müdahale etmemektedir.

3. Doğrulama ve kayıt fazında şifre, tek yönlü hash fonksiyonu tarafından korunarak (*pre-image resistance*) sunumcuya iletildiği için şifre, sistem yöneticisi tarafından görülmemektedir.

4. Şifreler düz metin halinde güvensiz ağda iletilmediğinden yoldaki herhangi bir saldırıda şifre çalınması olası değildir (man in the middle, eavesdropping).

5. Doğrulama fazında kullanıcı yanlış şifre girdiğinde uzak sisteme erişilmeden akıllı kartta kolaylıkla yanlış şifre tespiti yapılmaktadır.

6. Tahmin saldırıları çevrimiçi ve çevrim dışı tahmin saldırısı olmak üzere ikiye ayrılır. Çevrim içi tahmin saldırısı (Online Guessing Attack) yanlış şifre girişinin sayısını sınırlandırarak kolaylıkla engellenilebilir. Önerilen yöntemde üç yanlış deneme sonunda akıllı kart bloke edilerek sisteme giriş engellenmektedir. Çevrim dışı tahmin saldırılarında ise, Sunumcu, kayıt fazında kullanıcının tanımlayıcısını (ID), V değerinin içinde saklar ve şifreyi de tek yönlü özetleme fonksiyonu ile korur. Bu şekilde Çevrim dışı tahmin saldırılarına (Offline Guessing attack) karşı güvenlik sağlanmış olur.

7. Doğrulama esnasında hem sunumcu hem de kullanıcı birbirini doğrular böylece çift taraflı doğrulama yapılmış olur. Ve sunumcu aldatması (server spoofing) saldırılarına karşı güvenlik sağlanmış olur.

8. Önerilen yöntem, tekrarlı gönderme saldırılarına karşıda güvenilirdir. Doğrulama fazında her oturum için rasgele N_i ve N_s değeri üretildiği ve güvensiz ağda iletilmediği için saldırganın bir önceki bağlantıdan elde ettiği veriler ile farklı bir oturumda sisteme bağlanması mümkün değildir. Rasgele üretilen sayılar Açık anahtarlar hesaplanırken kullanılır (P_i , P_s) ve Bu değerlerden tekrar elde edilmesi ECDH ye göre verimli değildir. Ayrıca zaman eşleme problemini önlemek için zaman mührü kullanımına gidilmemiştir.

9. Şifre Değiştirme fazında eğer kullanıcı yanlış şifre girerse tespiti akıllı kartta yapılır. Akıllı kartın çalınması durumunda hiç kimse eski şifreyi bilmeden şifreyi değiştiremez. Bu sayede Akıllı kart çalınarak yapılan servis durdurma saldırılarına karşı güvenlik sağlanmaktadır

5. SONUÇ VE GELECEK ÇALIŞMALAR

Günümüzde internet uygulamalarının artmasından dolayı uzaktan kimlik doğrulama, sistemin güvenilirliğini ve bütünlüğünü sağlamak anlamında daha da önem kazanmıştır. Bu sebepten dolayı ideal bir kimlik doğrulama yöntemi oluşturulması amaçlı birçok çalışma yapılmıştır.

Bu tez çalışmasında uzaktan kimlik doğrulama için önerilen birçok yöntem bölüm 2.2 de incelenmiştir. Liaw ve diğ. yönteminin eksik yönleri geliştirilerek yeni bir yöntem önerilmiştir. Liaw ve diğ. yönteminin sahip olduğu güvenlik özellikleri korunarak, bazı kontroller ve eliptik eğri Diffie Hellman anahtar değişim protokolü eklenmiştir. Önerilen yöntemde eliptik eğri kriptografisi yöntemiyle doğrulama ve oturum anahtarı üretimi yapılmıştır. Geleneksel kriptosistemler yerine ECDH'nin kullanılmasının amacı daha küçük anahtar boyutu ile eş seviyede güvenlik sağlamasıdır ki buda daha az hafıza ve bant genişliğine karşılık gelmektedir. Daha önceden de belirtilen önerilen yöntem güvenlik özellikleri özetle: doğrulama tablosu gerekmemektedir, kullanıcı güvenli bir şekilde şifresini seçebilir ve değiştirebilir, oturum anahtarı ECDH kullanılarak doğrulama fazında üretilmiştir, iki taraflı doğrulama sağlanmaktadır ve yöntemin güvenliği tek kullanımlık rasgele üretilen sayıya, seçilen özetleme fonksiyonuna ve ECDH 'ye dayanmaktadır.

Gelecek çalışmalar için ECDH de kullanılan skaler nokta çarpımı için hesaplama maliyeti düşürülebilir.

KAYNAKLAR

Chang C.C., Wu T.C. Remote Password Authentication with Smart Cards. IEE proceedings-e;1991 Vol.138, p.165–168.

Chien H.Y.,Jan J.K.;Tseng Y.M. An efficient and practical solution to remote authentication:smart card; Computers & Security, 2002 vol.21,no.4, p.372-375.

Das M. L., Saxena A.,Gulati V.P. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics; 2004. vol. 50. no. 2. p. 629–631.

Diffie W., Hellman M.E. New directions in cryptography. IEEE Transactions on Information Theory; 1976. Vol. 22. p. 644 – 654.

Durlanik A., Soğukpınar I.SIP Authentication Scheme Using ECDH. Enformatika; 2005.Vol. 8, p. 350-353.

Gupta V., Gupta S., Chang S. Performance Analysis of Elliptic Curve Cryptography for SSL.In: ACM Wksp. Wireless Security, Mobicom, Atlanta.; 2002

Hwang M.S., Lee C.C., Tang Y.L. A simple remote user authentication .Math Comput Model 2002;36:103-7

Hwang M.S., Li L.H. A new remote user authentication scheme using smart cards. IEEE Transaction on consumer electronics; 2000. vol. 46, p. 28-30.

Ku W.C., Chen S.M. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics; 2004. vol. 50 no. 1 p. 204–207.

Lamport L. Password authentication with insecure communication. Communications of the ACM 24; 1981. p.770–772.

Lee C.C., Hwang M.S., Yang W.P. A Flexible Remote User Authentication Scheme Using Smart Cards. ACM Operating Systems Review; 2002 vol. 36, no3, p. 46-52.

Lee S.W., Kim H.S., Yoo K.Y. Comment on 'a remote user authentication scheme using smartcards with forward secrecy'. IEEE Transactions on Consumer Electronics; 2004 Vol.50 p.576 – 577.

Liao I-En, Lee C. C., Hwang M. S., Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme. In: IEEE CS Press Seoul, Korea; 2005. p. 437–440.

Liao I-En, Lee C. C., Hwang M. S. A password authentication scheme over insecure networks. Journal of Computer and System Sciences; 2006. p. 727-740.

Liaw H.T., Lin J.F., Wu W.C. An efficient and complete remote user authentication scheme using smart cards. Mathematical and Computer Modeling; 2006. p. 223-228

Lopez J., Dahab R. Fast Multiplication on Elliptic Curves over $GF(2^m)$ without Precomputation. LNCS;1999 p. 316-327.

NIST, "Recommended Elliptic Curves for Federal Government Use ", <http://csrc.nist.gov/csrc/fedstandards.html> July 1999.

Sun H.M, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics; 2000.Vol. 46.no.4 p. 958–961.

Tsai C.S., Lee C.C., Hwang M.S. Password Authentication Schemes: Current Status and Key issues. International Journal of Network security; 2005.Vol.3 No.2, p.101-115.

Yoon E. J., Ryu E. K., Yoo K. Y., An improvement of Hwang-Lee-Tang's simple remote user authentication schemes. Computers & Security; 2005. vol. 24 p. 50–56.

Yoon E. J., Ryu E. K., Yoo K. Y. Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics; 2004.Vol. 50. p. 612–614.

Yoon E. J., Ryu E. K., Yoo K. Y., Secure User Authentication Scheme Using Hash Function. ACM SIGOPS Operating Systems Review; 2004 Vol.38, p. 62 – 68.

Wang X.-M. et al. Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Computer Standards & Interfaces; 2006. doi:10.1016 /j.csi.2006. 11.005.

Wang X.G., Chai Z.C. Two Secure Remote User Authentication Schemes Using Smart Cards. Machine Learning and Cybernetics IEEE; 2006 p.2653–2658.

Wei Y.Z., Hu Y.P. Security Analysis of Timestamp-based Remote User Authentication Scheme Using Smart Cards. Communications, Circuits and Systems Proceedings; 2006 Vol. 3, p.1580-1582

Wenbo M., Modern Cryptography Theory and practice. Prentice Hall; 2004.

Wu W.C., Chiang M.H., Chang S.T. Weaknesses of Yoon- Ryu- Yoo's hash-based password authentication scheme. Operating systems review ISSN 0163-5980; 2005. vol. 39. p. 85-89.

ÖZGEÇMİŞ

1982 yılında Trabzon’da doğdu. Lise eğitimini İzmit Gazi Lisesi’nde tamamlayarak 1999 yılında Karadeniz Teknik Üniversitesi Biyoloji öğretmenliği Bölümü’ne girdi. 2001 yılında KTÜ’den ayrıldı ve Doğu Akdeniz Üniversitesi Bilgi Teknolojileri Bölümü’ne girdi. 2005 yılında mezun oldu ve Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü’nde yüksek lisans eğitimine başladı. Halen Yaşar Üniversitesi Bilgisayar Mühendisliği Bölümü’nde araştırma görevlisi olarak çalışmaktadır.